ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ
ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΟΛΥΕΠΙΠΕΔΟ ΣΧΕΣΙΑΚΟ ΜΟΝΤΕΛΟ ΕΚΤΙΜΗΣΗΣ ΚΙΝΔΥΝΟΥ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΔΙΕΞΑΓΩΓΗ ΕΡΓΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

του

ΔΙΟΝΥΣΙΟΥ ΚΕΦΑΛΛΗΝΟΥ

Διπλωματούχου Ηλεκτρολόγου Μηχανικού Ε.Μ.Π.

Ζωγράφου, Ιούνιος 2012

Η σελίδα αυτή είναι σκόπιμα λευκή

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ
ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΟΛΥΕΠΙΠΕΔΟ ΣΧΕΣΙΑΚΟ ΜΟΝΤΕΛΟ ΕΚΤΙΜΗΣΗΣ ΚΙΝΔΥΝΟΥ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΔΙΕΞΑΓΩΓΗ ΕΡΓΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

του

ΔΙΟΝΥΣΙΟΥ ΚΕΦΑΛΛΗΝΟΥ

Διπλωματούχου Ηλεκτρολόγου Μηχανικού Ε.Μ.Π.

Συμβουλευτική Επιτροπή: Ε. Συκάς (επιβλέπων)
Μ. Αναγνώστου
Α.-Γ. Σταφυλοπάτης

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 29 Ιουνίου 2012

.....	.....	.....
Ευστάθιος Συκάς	Μιλτιάδης Αναγνώστου	Ανδρέας-Γεώργιος Σταφυλοπάτης
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.
.....	.....	.....
Μιχαήλ Θεολόγου	Συμεών Παπαβασιλείου	Βασίλειος Βεσκούκης
Καθηγητής Ε.Μ.Π.	Αν. Καθηγητής Ε.Μ.Π.	Επ. Καθηγητής Ε.Μ.Π.

.....
Μαρία Λάμπρου
Επ. Καθηγήτρια Παν. Αιγαίου

Ζωγράφου, Ιούνιος 2012

……
Διονύσιος Κεφαλληνός
Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Για τις αναφορές έχει ακολουθηθεί το πρότυπο American Psychology Association, έκδοση 6η.

ΕΥΧΑΡΙΣΤΙΕΣ

Θερμές ευχαριστίες στον Καθ. Ε.Μ.Π. Ευστάθιο Συκά, τον κύριο λόγο ολοκλήρωσης αυτής της διατριβής.

Ευχαριστίες στην Επ. Καθ. Παν. Αιγαίου Μαρία Λάμπρου για τις ιδέες της.

Ευχαριστίες στη σύζυγο μου Ερ. Δρ. Νίκη Βασιλάκη, χωρίς την ανοχή και την υποστήριξη της οποίας δεν θα ήταν δυνατή η ολοκλήρωση της διατριβής.

Αφιερωμένη στην κόρη μου, Ερμιόνη-Νικολέτα.

Η σελίδα αυτή είναι σκόπιμα λευκή

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΠΕΡΙΛΗΨΗ ΔΙΑΤΡΙΒΗΣ

Σε αυτή τη διατριβή προτείνεται μια πρωτότυπη μεθοδολογία Αξιολόγησης Διακινδύνευσης (ΑΔ) και ένα αντίστοιχο εργαλείο εφαρμογής, τα οποία απευθύνονται ειδικά σε έργα Ηλεκτρονικής Διακυβέρνησης (ΗΔ), παρέχοντας ωστόσο τη δυνατότητα προσαρμογής και εφαρμογής και σε άλλους τομείς ΑΔ. Η μεθοδολογία φιλοδοξεί να διαφέρει από τις συμβατικές, στο πεδίο εφαρμογής της, στον τρόπο που εφαρμόζεται, στον τρόπο που εξάγει τα αποτελέσματα και στις μεθόδους που προτείνει για τη μείωση της επικινδυνότητας των έργων και συστημάτων στα οποία εφαρμόζεται.

Περιγράφεται το περιβάλλον που αναπτύχθηκε, καθώς και τα κίνητρα και η εμπειρία που ώθησαν στην ανάπτυξή της. Γίνεται αναλυτική περιγραφή της μεθοδολογίας και του αλγόριθμου εφαρμογής της, όπως και του τρόπου εξαγωγής των αποτελεσμάτων. Το εργαλείο εφαρμογής περιλαμβάνει εκτενή βιβλιοθήκη επιπέδων, περιοχών και διαστάσεων κινδύνου, καθώς και αντιμέτρων και κρισίμων παραγόντων επιτυχίας. Παρέχονται τρόποι υπολογισμού των πιθανοτήτων και των επιπτώσεων των κινδύνων, του κόστους των αντιμέτρων και της εκτίμησης κάλυψης αυτών, καθώς και σειρά δεικτών που χρησιμοποιούνται για την εξαγωγή συμπερασμάτων διακινδύνευσης, συνολικής κάλυψης κινδύνου, περιθωρίου κάλυψης και κόστους αντιμέτρων. Η μεθοδολογία περιλαμβάνει πρόβλεψη για αλληλεξαρτήσεις κινδύνων και έργων με χρήση Bayesian Belief Networks και τρισδιάστατες μήτρες. Για να δειχθεί ο τρόπος χρήσης της και η χρησιμότητα των αποτελεσμάτων που εξάγει, εφαρμόζεται σε δύο έργα υποδομής δημοσίου κλειδιού (ΥΔΚ), ένα που έχει υλοποιηθεί και ένα που έχει προταθεί για υλοποίηση.

Το κίνητρο για την ανάπτυξη της προτεινόμενης μεθοδολογίας εκπήγασε από μακρόχρονη εμπειρία και παρατήρηση στο πεδίο της ΑΔ, της ΗΔ και των έργων στον ευρύτερο δημόσιο τομέα. Σε αυτό το πεδίο, η έλλειψη διάδρασης μεταξύ των τεχνικών μεθοδολογιών (όπως και των τεχνικών εμπειρογνωμόνων και ερευνητών) και πλαισίων/προτύπων Διοίκησης Τεχνολογίας Πληροφορίας (ΔΤΠ) (και διευθυντικών/διοικητικών στελεχών), είναι συνήθης, ιδιαίτερα σε έργα όπου συμμετέχουν και αλληλεπιδρούν δημόσιοι οργανισμοί, ο ιδιωτικός τομέας και το ευρύτερο κοινό. Από την άλλη πλευρά, η υιοθέτηση και υλοποίηση προτύπων ασφάλειας και διαδικασιών και πλαισίων ΗΔ πολλές φορές μένει στα χαρτιά και εν τέλει σπάνια βοηθά πραγματικά στην επιτυχή ολοκλήρωση των έργων. Επιπλέον, μεγάλος αριθμός σημαντικών έργων/συστημάτων αποτυγχάνουν στους στόχους τους και τη λειτουργία τους, όχι τόσο λόγο βασικών κοινωνικών εμποδίων (κάτι που επίσης συμβαίνει συχνά, παρότι στοι-

χειώδες), όσο λόγω βασικών ελλείψεων και εμποδίων στο άμεσο περιβάλλον υλοποίησής τους.

Υπό αυτές τις συνθήκες παρουσιάζεται σημαντικός αριθμός προβληματικών σημείων, τόσο στις φάσεις ανάπτυξης και εφαρμογής, όσο και στην παραγωγική λειτουργία και στην τελική υιοθέτηση των νέων υπηρεσιών από τους στοχευόμενους χρήστες, με αποτέλεσμα την υποβάθμιση της σημαντικότητας, της εμπιστοσύνης και της αποδοχής των αποτελεσμάτων και των υποδείξεων της ΑΔ (τα οποία είναι ούτως ή άλλως περιορισμένου πεδίου λόγω των μη ειδικευμένων εργαλείων) και τελικά και του ίδιου του έργου στο σύνολό του.

Η μεθοδολογία ΑΔ που μοντελοποιείται και αναπτύσσεται σε αυτή τη διατριβή μπορεί να θεωρηθεί ως μια προέκταση υπαρχουσών τεχνικών εκτίμησης κινδύνου τεχνολογικών έργων και συστημάτων, προσβλέποντας στο:

α) να αποτελέσει μια γρήγορη, εύκολη και αποτελεσματική μεθοδολογία και εργαλείο, ειδικευμένα στο πεδίο τους,
β) να ανταποκριθεί καλύτερα στους στόχους ασφάλειας και προστασίας προσωπικών δεδομένων σε έργα ΗΔ, παρέχοντας καλύτερη υποστήριξη στη μορφοποίηση και επιτέλεση αποφάσεων σχετικών με την ασφάλεια,
γ) να παρέχει μια σύνδεση ανάμεσα σε τεχνολογικές μεθοδολογίες ΑΔ και πλαίσια ΔΤΠ,
δ) να αυξήσει την εξοικείωση σε θέματα ασφάλειας και προστασίας του απορρήτου, προωθώντας την ενεργό συμμετοχή μεγάλης γκάμας μη τεχνικού προσωπικού,
ε) να ενισχύσει την υλοποίηση βασικών πολιτικών ασφάλειας και προστασίας του απορρήτου,
στ) να ενσωματώσει μακρόχρονη και πολυποίκιλη εμπειρία και έρευνα στις δομές και τις διαδικασίες εκτέλεσης έργων στη δημόσια διοίκηση, έτσι ώστε να αποτελέσει ένα αποτελεσματικό αρωγό για την επιτυχία των έργων και
ζ) να διαθέτει λογική και διεργασίες που να μπορούν, με κατάλληλες αλλαγές να εφαρμοστούν και σε άλλους τομείς ΑΔ.

Σε εκ των υστέρων εφαρμογή της μεθοδολογίας σε έργα ΗΔ, βρέθηκε ότι καλύπτει ικανοποιητικά τους συνήθεις κινδύνους για την επιτυχή υλοποίηση και αποδοχή των έργων και ότι βοηθά στον αυτοέλεγχο της αξιολόγησης και στην επίγνωση των σημαντικών παραγόντων. Οι δύο εφαρμογές της μεθοδολογίας που παρουσιάζονται αφορούν

ΥΔΚ, έργα που αποτελούν συνήθεις περιπτώσεις αποτυχίας όταν εφαρμόζονται σε μεγάλη κλίμακα, σε ιδιωτικό ή εθνικό επίπεδο, εντός και εκτός Ελλάδος. Και οι λόγοι της αποτυχίας τους (η οποία συνίσταται τυπικά σε αποτυχία διείσδυσης στο στοχευόμενο κοινό), είναι επίσης χαρακτηριστικές περιπτώσεις πραγμάτωσης των κινδύνων που αξιολογεί η προτεινόμενη μεθοδολογία. Το ένα είναι η ΥΔΚ-ΣΥΖΕΥΞΙΣ, ένα έργο που μελετήθηκε και υλοποιήθηκε υποδειγματικά, για να μην επιτύχει όμως τελικά τους στόχους που φιλοδοξούσε σε πλάτος χώρου και βάθος χρόνου. Το έργο αυτό αποτέλεσε ένα από τα κίνητρα που οδήγησαν στην ανάπτυξη της προτεινόμενης μεθοδολογίας. Το δεύτερο έργο είναι μια πρωτότυπη ΥΔΚ που προστατεύει το απόρρητο προσωπικών πληροφοριών (ιδιοαπόρρητο) και την ελευθερία βούλησης των χρηστών της. Η αρχική επιδίωξη ήταν να αποτελέσει μια παραδειγματική περίπτωση εφαρμογής της προτεινόμενης μεθοδολογίας, διαθέτοντας όλα τα «επικίνδυνα» χαρακτηριστικά που πραγματεύεται η προτεινόμενη μεθοδολογία. Ο πρωτότυπος όμως τρόπος αντιμετώπισης της προστασίας του ιδιοαπόρρητου που εισάγει, οδήγησε σε τελικά μια υποδειγματική καθεαυτό ΥΔΚ, η οποία προτάθηκε για δημοσίευση.

Τα αποτελέσματα των δύο εφαρμογών ήταν σημαντικά για την αξιολόγηση της χρησιμότητας και της αποτελεσματικότητας της προτεινόμενης μεθοδολογίας. Συνοψίζοντας, μπορούν να εξαχθούν τα ακόλουθα συμπεράσματα γι' αυτήν:

α) Επιτυγχάνει τους κύριους στόχους της που είναι να οδηγήσει τους αξιολογητές σε μια συστηματική μέθοδο αξιολόγησης, να καταδείξει σημαντικούς κινδύνους που θα πρέπει να λάβουν υπόψη τους, να προτείνει αποτελεσματικά αντίμετρα προς υιοθέτηση και να εξάγει χρήσιμα αποτελέσματα εκτίμησης κινδύνου.

β) Αποτελεί ένα συνεκτικό εργαλείο χωρίς κενά και υποβοηθά τους αξιολογητές με σημαντικό υλικό για την ολοκλήρωση μιας χρήσιμης και αποτελεσματικής αξιολόγησης.

γ) Αποτελεί μια ευέλικτη μεθοδολογία που μπορεί να προσαρμοστεί σύμφωνα με την κρίση των αξιολογητών με προσθαφαίρεση στοιχείων, παραγόντων και δεδομένων σε όλα της τα δομοστοιχεία (κίνδυνοι και επίπεδα κινδύνων, ΚΠΕ, αντίμετρα, εκτίμηση επίπτωσης, παραγόντων πρόκλησης, αποτελεσμάτων πραγμάτωσης, τρωτοτήτων, ενδεχομένων αντίστροφης πραγμάτωσης). Με αλλαγή στους κίνδυνους, στους ΚΠΕ και τα αντίμετρα μπορεί να εφαρμοστεί ακόμα και σε άλλα πεδία ΑΔ.

δ) Με προσοχή στην εξαγωγή συμπερασμάτων μπορούν να αξιολογηθούν ακόμα και μεμονωμένα επίπεδα διακινδύνευσης του υπό εξέταση έργου/συστήματος.

ε) Όπως όλες οι μεθοδολογίες ΑΔ, εξαρτάται σε σημαντικό βαθμό από την ικανότητα των αξιολογητών που την εφαρμόζουν, ώστε να παράγει χρήσιμα αποτελέσματα με νόημα.

στ) Όπως όλες οι μεθοδολογίες ΑΔ, απαιτεί σημαντική προσπάθεια και χρόνο για την αναλυτική εφαρμογή της. Αυτό μπορεί να μειωθεί σε αρκετό βαθμό αν γίνει προσεγγιστική ή/και κατ' εκτίμηση τοποθέτηση των πιθανοτήτων πραγμάτωσης των κινδύνων, των επιπτώσεών τους και της κάλυψης των αντιμέτρων (για όλα ή για κάποια από αυτά) και όχι ο αναλυτικός υπολογισμός που περιγράφεται. Και πάλι, αυτό εξαρτάται από την κρίση, την εμπειρία και ικανότητα των αξιολογητών που την εφαρμόζουν.

Επομένως, η προτεινόμενη μεθοδολογία ΑΔ μπορεί να αποτελέσει αποτελεσματικό αρωγό για την επιτυχία των έργων, με το μοναδικό μειονέκτημα, λόγω της (προς το παρόν) μη υλοποίησης της σε λογισμικό, μιας σχετικά χρονοβόρας διαδικασίας εφαρμογής. Η καινοτομία της προσέγγισής της βρίσκεται:

α) Στην ενσωμάτωση μεγάλου αριθμού μη συμβατικών και μη τεχνικών παραγόντων κινδύνου, αλλά σχετικών με την ΗΔ και συχνά εμφανιζόμενων, από περιοχές όπως η κοινωνία, οι τελικοί χρήστες, η δημόσια διοίκηση, οι πολιτική, το νομικό και κανονιστικό πλαίσιο, ακόμα και η ψυχολογία, σε μια εύκολη στη χρήση επαναληπτική διαδικασία ΑΔ.

β) Στην εξαγωγή αποτελεσμάτων με χρήση πρακτικών, δεκτικών σε συγκριτικές διαδικασίες και περιληπτικών δεικτών διακινδύνευσης.

γ) Στη διαφορετική προσέγγισή της στην ΑΔ συστημάτων και έργων ΗΔ. Ακολουθώντας διαφορετική φιλοσοφία από τις συμβατικές τεχνικές μεθοδολογίες και εργαλεία (τα οποία προσανατολίζονται περισσότερο προς τις τεχνικές λεπτομέρειες), ενσωματώνει ειδικότερα περιοχές διακινδύνευσης ιδιαίτερα σημαντικές στο πεδίο των έργων ΗΔ, οι οποίες αποτελούν πιο συνήθεις λόγους αποτυχίας των. Αποτελεί έτσι μια διεπαφή ανάμεσα στην ευρύτερη τεχνοκρατική διοικητική φιλοσοφία των COBIT, ISO/IEC 27002 και ITIL και των τεχνικών μεθοδολογιών ΑΔ, προσθέτοντας και αναδεικνύοντας νέες διαστάσεις, στις οποίες πρέπει να κατευθυνθεί η προσοχή προσώπων-κλειδιά έργων ΗΔ, έτσι ώστε να κινήσουν τις αντίστοιχες δράσεις και να λάβουν τα απαραίτητα μέτρα.

δ) Στην προαγωγή του αυτοέλεγχου και της αυτοαξιολόγησης της διαδικασίας ΑΔ, πέρα από τα όρια των τεχνικών εργαλείων και εντός της περιοχής των πλαισίων ΔΤΠ και των αποτελεσματικών πρακτικών ΗΔ.

ε) Στη μεγάλη ευελιξία. Οι αξιολογητές μπορούν να επιλέξουν (και να προσθαφαιρέσουν) από τα στοιχεία που παρέχει η μέθοδος αυτά που επιθυμούν, χωρίς να επηρεάζεται η δυνατότητά της να εξάγει αποτελέσματα. Ασφαλώς, όσο πιο πλήρη είναι τα στοιχεία που θα επιλεγούν, όσο καλύτερα καλύπτουν την περίπτωση εφαρμογής, τόσο πιο αξιόπιστα θα είναι τα αποτελέσματα. Ωστόσο οι αξιολογητές μπορούν να επιλέξουν τους κινδύνους που θα αξιολογήσουν, τα αποτελέσματά τους σε περίπτωση πραγμάτωσης, τους παράγοντες που μπορεί να τους προκαλέσουν, τις τρωτότητες του έργου που μπορεί να αποτελέσουν σημεία τρώσης και από αυτές την κάλυψη των αντιμέτρων. Η προτεινόμενη μεθοδολογία επομένως διαθέτει την ευελιξία για να εφαρμοστεί σαν σχεδιότυπο ουσιαστικά σε οποιοδήποτε είδος συστήματος, σε οποιοδήποτε τομέα ΑΔ.

Οι παράγοντες που επηρεάζουν την επιτυχή εφαρμογή και την εξαγωγή ορθών αποτελεσμάτων της ίδιας της μεθοδολογίας συνίστανται:

α) Στην επιλογή όλων των σημαντικών για το έργο κινδύνων, ακόμα και πέρα, αν απαιτείται, από αυτούς που προτείνονται, σύμφωνα με την κρίση των αξιολογητών.

β) Στη συμπερίληψη των απαραίτητων για τους σκοπούς του έργου κρίσιμων παραγόντων επιτυχίας (ΚΠΕ), και

γ) Στην επιλογή αποτελεσματικών, εφικτών και οικονομικά αποδοτικών αντιμέτρων που δεν αποβαίνουν σε βάρος της λειτουργικότητας και της φιλικότητας του συστήματος.

Η κύρια αδυναμία της μεθοδολογίας, στην τρέχουσα μορφή της, είναι ότι η απόδοση και η αποτελεσματικότητά της εξαρτάται από την αποφασιστικότητα, τη διορατικότητα και την εμπειρία των επαγγελματιών που θα το χρησιμοποιήσουν (κάτι που ισχύει όμως ούτως ή άλλως για όλες τις μεθοδολογίες και εργαλεία ΑΔ), μαζί με άλλα περισσότερο καθιερωμένα εργαλεία. Αυτό διότι, αν και αποτελεί ένα ολοκληρωμένο εργαλείο με πλήρεις βιβλιοθήκες στοιχείων, δεν είναι στην τρέχουσα μορφή του υλοποιημένο σε λογισμικό, έτσι ώστε πλήρως αυτόνομα να μπορεί να εξασφαλίσει λεπτομερή προσέγγιση της ασφάλειας, συστηματική αξιολόγηση των υποστοιχείων των έργων και

ολοκληρωμένη τεκμηρίωση των πολιτικών και των μέτρων που πρέπει να εφαρμοστούν.

Η ανάπτυξη της μεθοδολογίας σε λογισμικό, με βάση γνώσης για τους κινδύνους, τους ΚΠΕ και τα αντίμετρα, έτοιμα εργαλεία κατασκευής γράφων αλληλεξαρτήσεων, υπολογισμού των πιθανοτήτων και αναφορών, καθώς και διεπαφές με εμπορικά συστήματα ΑΔ θα αποτελέσει αντικείμενο περαιτέρω εξέλιξης με σκοπό την εμπορική εκμετάλλευση.

Ως αντικείμενο περαιτέρω έρευνας προτείνεται η διαμόρφωση της μεθοδολογίας σε σχεδιότυπο για εφαρμογή σε άλλα πεδία εφαρμογής ΑΔ. Προσαρμόζοντας τις περιοχές κινδύνου, τους ΚΠΕ και τα αντίμετρα, ο αλγόριθμος και οι δείκτες της μεθοδολογίας μπορούν να εφαρμοστούν κατάλληλα, ώστε να αποτελέσουν χρήσιμο εργαλείο και σε άλλους τομείς, τεχνολογικούς και μη, όπως βιολογικά συστήματα, οικοσυστήματα, κοινωνικές δομές κ.ά.

ABSTRACT

In this dissertation we propose a novel risk assessment (RA) methodology and a corresponding implementation tool, which are directed specifically towards electronic governance (EG) initiatives, while providing the possibility of adaptation and implementation in other RA scopes. The methodology aspires to differ from the conventional ones, in its field of implementation, on the way it is applied, on the way it forms its results and in the methods it proposes to mitigate risk on the projects and systems it is implemented.

We describe its background and the motives and experiences that led us to develop it. We analyze the methodology and its implementation procedure, as well as the way results are extracted. The implementation tool incorporates a broad library of levels, areas and dimensions of risk, as well as countermeasures and critical success factors. We provide ways of calculating the probabilities and the impact of the risks, the cost of the countermeasures and their coverage of risk, as well as a series of indices used to express inferences about risk, total coverage, margin of coverage and countermeasure cost. The methodology provisions for risk and project dependencies, employing Bayesian Belief Networks and three dimensional matrices. In order to demonstrate its usage and the usefulness of its results, it is implemented in two public key infrastructure (PKI) projects, one that has already been implemented and one that is proposed for implementation.

The proposed methodology aspires to:

a) Be a quick, easy and effective RA methodology and tool, specialized in its field,
b) To better target the security and privacy goals in e-government projects, since a contextualized tool promotes improved formulation and facilitation of accurate security-related decisions,
c) To form a connection between technical ICT RA methodologies and Information Technology Governance (ITG) frameworks,
d) To increase security and privacy awareness by promoting the active involvement of a larger variety of non-technical personnel,
e) To facilitate the application of baseline security and privacy policies,
f) To integrate long term and diverse experience and research in public administration project structures and procedures, so as to be an effective aid in project success and

g) To have logic and processes that can be adapted and implemented to other RA fields.

The novelty of its approach lies in:

a) Its integration of a large number of unconventional, non-technical, but common EG-related risk factors, from areas such as the society, the end-users, the public administration personnel, politics, legal and regulatory frameworks, even psychology, in an easy to use iterative RA process.
b) The expression of its results using practical, comparison-friendly and succinct risk indices.
c) Its diverse approach to EG systems and projects RA. Following a dissimilar philosophy than conventional RA methodologies and tools (which focus mainly on technical issues and processes), it specifically incorporates areas of risk particularly important in EG, which constitute the most common causes for failure. It attempts to provide an interface between the broader managerial philosophy of COBIT, ISO/IEC 27002 and ITIL and the technical methodologies, by adding and integrating dimensions, upon which the attention of key EG stakeholders can be drawn and respective actions or measures can be undertaken.
d) Its promotion of self-check and self-evaluation of the RA process, beyond the limits of technical tools and into the realm of information technology governance (ITG) frameworks and effective EG practices.
e) In its great flexibility. The evaluators can choose (and add/subtract) from the elements provided those that they wish, without inhibiting the methodology's ability to extract results. Naturally, the more comprehensive they are and the better they cover the case study, the more trustworthy the results are. However, the evaluators can choose the risks they evaluate, the results in case of their fulfillment, the factors that may cause them, the vulnerabilities that may be affected by them and the coverage of the countermeasures. As a result, the proposed methodology possesses the flexibility to be used as a template in virtually any kind of system, in any area of RA.

The critical success factors (CSFs) of the methodology itself and its ability to extract useful results are:

a) The inclusion in the evaluation of the all the important for the project risk factors, even beyond, if necessary, the ones proposed in the methodology, according to the judgment of the evaluators.
b) The inclusion of all the essential, for the purposes of the project, CSFs and
c) The selection of effectual, attainable and cost-effective countermeasures that do not operate against the functionality and friendliness of the system.

The main weakness of the methodology, in its current form, is that its performance and effectiveness rests upon the determination, insight and experience of the professionals who will use it (which is true for all RA methodologies and tools anyway), complementary to other more established toolkits. This because, while it comprises a complete tool with a rich library of data, it is not currently implemented in software, so as to autonomously guide and assist in a systematic evaluation, determine a detailed security approach for assets needing protection and suggest the security policies to apply.

As further development, we intent to implement the methodology as a software toolkit, with a knowledge base for the risks, CSFs and countermeasures, tools for dependency graph construction, probabilities calculation and reports, as well as an interface with other well-known toolkits.

As a subject of further research, we suggest the formation of the methodology into a template, for application in other areas of RA. Adjusting the risk areas, the CSFs and the countermeasures, the application algorithm and the risk indices can be fitted appropriately, so as to consist a useful tool in other fields, technological and non-technological, such as biological systems, ecosystems, social structures etc.

Η σελίδα αυτή είναι σκόπιμα λευκή

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Η σελίδα αυτή είναι σκόπιμα λευκή

Σε αυτό το κεφάλαιο της διατριβής, ορίζεται αρχικά το πρόβλημα που θα αντιμετωπιστεί και τίθενται οι στόχοι που φιλοδοξεί να πετύχει η προτεινόμενη μεθοδολογία. Ορίζεται οι έννοια της αξιολόγησης διακινδύνευσης, η θέση της εντός των διαδικασιών ανάπτυξης, υλοποίησης και λειτουργίας ενός έργου και συνοψίζονται τα στοιχεία που περιλαμβάνουν τυπικά οι μεθοδολογίες αξιολόγησης διακινδύνευσης.

1.1 Ορισμός προβλήματος – στόχοι

Σε αυτή τη διατριβή προτείνεται μια πρωτότυπη μεθοδολογία Αξιολόγησης Διακινδύνευσης (ΑΔ) και ένα αντίστοιχο εργαλείο εφαρμογής, τα οποία απευθύνονται ειδικά σε έργα Ηλεκτρονικής Διακυβέρνησης (ΗΔ), διατηρώντας τη δυνατότητα προσαρμογής και εφαρμογής και σε άλλους τομείς ΑΔ.

Δεδομένης της μεγάλης ποικιλότητας εννοιών και εφαρμογών στην ΗΔ, το να δοθεί ένας πλήρης ορισμός της καθίσταται ολοένα και πιο δύσκολο (Roy, 2003). Γενικά, η ΗΔ αναφέρεται σε στρατηγικές, οργανωτικές δομές, διαδικασίες, αλλά και τεχνολογίες πληροφορικής και επικοινωνιών (ΤΠΕ) που αναπτύσσονται έτσι ώστε να μεγεθύνεται η πρόσβαση στην- και η χρήση της- πληροφορίας και υπηρεσιών της δημόσιας διοίκησης από τους πολίτες, τις επιχειρήσεις, τις δημόσιες υπηρεσίες και άλλους τρίτους. Από τεχνολογικής σκοπιάς, τα έργα ΗΔ περιλαμβάνουν εν γένει πολλά είδη ψηφιακής τεχνολογίας και πληροφοριακών συστημάτων, συμπεριλαμβανομένων βάσεων και εξόρυξης δεδομένων, δικτύωσης, συνεργατικών υπηρεσιών, πολυμέσων, παρακολούθησης και ιχνηλάτισης, καθώς και τεχνολογιών προστασίας του απορρήτου (Snellen, 2002). Εν γένει, μπορούμε να θεωρήσουμε τα έργα ΗΔ ως τεχνικά εγχειρήματα που προωθούν το σκοπό της μοντελοποίησης και απεικόνισης διαδικασιών Government-to-Government (G2G), Government-to-Business (G2B) και Government-to-Citizen (G2C) στον ηλεκτρονικό κόσμο, περιλαμβάνοντας και ενέχοντας (τόσο στην ανάπτυξή τους όσο και στη λειτουργία τους) δημόσιους υπάλληλους, ιδιωτικές εταιρίες, επαγγελματίες, αλλά και το ευρύτερο κοινό.

Τα σημαντικότερα θέματα και οι δυσκολίες για την επιτυχή σχεδίαση, ανάπτυξη, παράταξη και χρήση ασφαλών υποδομών ΗΔ (και γενικότερα υπηρεσιών ΤΠΕ), έχουν τεκμηριωθεί εκτενώς από ερευνητές (Curthoys & Crabtree, 2003; Gil-Garcia & Pardo, 2005; Jaeger, 2003; Löfstedt, 2005; Martin, 2005; Relyea, 2002; Vassilakis et al., 2005). Αυτοί υποδεικνύουν την έκταση των πολύπλοκων και πολυποίκιλων δυσκολιών που πρέπει να αντιμετωπιστούν από τους διαχειριστές και τους προγραμματιστές των έργων

στις φάσεις της σχεδίασης, ανάπτυξης και λειτουργίας τους. Και είναι γενικά αποδεκτό ότι η επιτυχής έκβασή τους δεν σχετίζεται τόσο με την επιλογή κατάλληλων τεχνολογιών, όσο με τη διαχείριση των οργανωτικών δυνατοτήτων, την αντιμετώπιση κανονιστικών περιορισμών και περιβαλλοντικών πιέσεων και την πρόβλεψη κοινωνικών, πολιτικών και ψυχολογικών προβλημάτων των ανθρώπων που εμπλέκονται. Με άλλα λόγια, εξαρτάται σημαντικά από την αποτελεσματική εκτίμηση των κινδύνων για την επιτυχή έκβαση του εγχειρήματος και των διοικητικών τεχνολογικών δομών, στα πλαίσια του περιβάλλοντος του έργου. Η αποδοτική και ασφαλής σχεδίαση, υλοποίηση και λειτουργία ενός πολύπλοκου πληροφοριακού και τηλεπικοινωνιακού συστήματος εξαρτώνται τελικά από την περιεκτική διασάφηση των στόχων, των λειτουργικών απαιτήσεων και της ασφάλειας, την ορθή και συνεπή μετατροπή τους σε πολιτικές, την αντίστοιχη ανάπτυξη του συστήματος και την επιβολή και παρακολούθηση αυτών των πολιτικών κατά τη λειτουργία του. Και αυτό πρέπει να ακολουθηθεί από μια αδιάκοπη διαδικασία προσαρμογής των πολιτικών σε μεταβαλλόμενα πλαίσια, περιβάλλοντα, κοινωνικές και οικονομικές συνθήκες, τεχνολογίες, τρόπους χρήσης και απειλές στην ασφάλεια.

Προκειμένου να γίνει δυνατή α) η κατανόηση των πολύπλοκων συσχετισμών μεταξύ των πολιτικών ασφάλειας, της υποδομής και των τρωτοτήτων, β) η επίτευξη και η επικύρωση των στόχων ασφάλειας, γ) η ανύψωση του επιπέδου ποιότητας και διαβεβαίωσης της διαδικασίας ΑΔ και τελικά δ) η αύξηση της εμπιστοσύνης σε αυτήν και στο υπό εξέταση σύστημα, απαιτούνται τυπικές (formal) και βασισμένες σε εργαλεία (tool-based) μεθοδολογίες, οι οποίες ως πρόσθετο όφελος, καθοδηγούν προς μια μεθοδική και συστηματική αξιολόγηση και βοηθούν στον προσδιορισμό του τι ακριβώς χρειάζεται προστασία και ποιες πολιτικές ασφαλείας πρέπει να εφαρμοστούν.

Το κίνητρο για την ανάπτυξη της προτεινόμενης σε αυτή τη διατριβή μεθοδολογίας εκπήγασε από μακρόχρονη εμπειρία και παρατήρηση στο πεδίο της ΑΔ, της ΗΔ και των έργων στον ευρύτερο δημόσιο τομέα. Σε αυτό το πεδίο, η έλλειψη διάδρασης μεταξύ των τεχνικών μεθοδολογιών (όπως και των τεχνικών εμπειρογνωμόνων και ερευνητών) και των πλαισίων/προτύπων διοίκησης τεχνολογίας πληροφορίας (ΔΤΠ) (και διευθυντικών/διοικητικών στελεχών), είναι συνήθης, ιδιαίτερα σε έργα όπου συμμετέχουν και αλληλεπιδρούν δημόσιοι οργανισμοί, ο ιδιωτικός τομέας και το ευρύτερο κοινό. Από την άλλη πλευρά, η υιοθέτηση και υλοποίηση προτύπων ασφάλειας και διαδικασιών και πλαισίων ΗΔ πολλές φορές μένει στα χαρτιά και εν τέλει σπάνια βοηθά πραγματικά στην επιτυχή ολοκλήρωση των έργων. Επιπλέον, μεγάλος αριθμός σημαντικών έργων/συστημάτων αποτυγχάνουν στους στόχους τους και τη λειτουργία τους, είτε (ακό-

μη χειρότερα) παραμένουν αχρησιμοποίητα, όχι τόσο λόγο ευρύτερων κοινωνικών αντιδράσεων (κάτι που επίσης συμβαίνει συχνά, παρότι στοιχειώδες), όσο λόγω βασικών ελλείψεων και εμποδίων στο άμεσο περιβάλλον υλοποίησής τους.

Υπό αυτές τις συνθήκες παρουσιάζεται σημαντικός αριθμός προβληματικών σημείων, τόσο στις φάσεις ανάπτυξης και εφαρμογής, όσο στην παραγωγική λειτουργία, όσο και στην τελική υιοθέτηση νέων υπηρεσιών από τους στοχευόμενους οργανισμούς και χρήστες, με αποτέλεσμα την υποβάθμιση της σημαντικότητας, της εμπιστοσύνης και της αποδοχής των αποτελεσμάτων και των υποδείξεων της ΑΔ (τα οποία είναι ούτως ή άλλως περιορισμένου πεδίου λόγω των μη ειδικευμένων εργαλείων) και τελικά και του ίδιου του έργου στο σύνολό του.

Η μεθοδολογία ΑΔ που μοντελοποιείται και αναπτύσσεται σε αυτή τη διατριβή μπορεί να θεωρηθεί ως μια προέκταση υπαρχουσών τεχνικών εκτίμησης κινδύνου τεχνολογικών έργων και συστημάτων, προσβλέποντας στο:

α) να αποτελέσει μια γρήγορη, εύκολη και αποτελεσματική μεθοδολογία και εργαλείο, ειδικευμένα στο πεδίο τους,
β) να ανταποκριθεί καλύτερα στους στόχους ασφάλειας και προστασίας προσωπικών δεδομένων σε έργα ΗΔ, παρέχοντας καλύτερη υποστήριξη στη μορφοποίηση και επιτέλεση αποφάσεων σχετικών με την ασφάλεια,
γ) να παρέχει μια σύνδεση ανάμεσα σε τεχνολογικές μεθοδολογίες ΑΔ και πλαίσια ΔΤΠ,
δ) να αυξήσει την εξοικείωση σε θέματα ασφάλειας και προστασίας του απορρήτου, προωθώντας την ενεργό συμμετοχή μεγάλης γκάμας μη τεχνικού προσωπικού,
ε) να ενισχύσει την υλοποίηση βασικών πολιτικών ασφάλειας και προστασίας του απορρήτου,
στ) να ενσωματώσει μακρόχρονη και πολυποίκιλη εμπειρία και έρευνα στις δομές και τις διαδικασίες εκτέλεσης έργων στη δημόσια διοίκηση, έτσι ώστε να αποτελέσει ένα αποτελεσματικό αρωγό για την επιτυχία των έργων και
ζ) να διαθέτει λογική και διεργασίες που να μπορούν, με κατάλληλες αλλαγές να εφαρμοστούν και σε άλλους τομείς ΑΔ.

Στο υπόλοιπο του κεφαλαίου αυτού ορίζεται κατ' αρχήν η έννοια της ΑΔ, τα στοιχεία που περιλαμβάνει τυπικά και η τοποθέτησή της εντός της μελέτης ασφάλειας ενός

συστήματος/έργου. Περιγράφονται επίσης οι κρίσιμοι παράγοντες για την επιτυχία της και τα οφέλη από την αρχική και την επαναληπτική εφαρμογή της.

Στο δεύτερο κεφάλαιο της διατριβής, παρατίθενται γνωστές μεθοδολογίες γενικής ΑΔ που χρησιμοποιούνται σε πλήθος τομέων της βιομηχανικής παραγωγής, καθώς και μεθοδολογιών για πληροφοριακά συστήματα και ηλεκτρονικές υπηρεσίες. Συνεχίζοντας, παρουσιάζονται γνωστά πλαίσια ΔΤΠ και το τι έχουν αυτά να προσφέρουν τόσο στην οργάνωση, όσο και στην ανάλυση της ασφάλειας των διαδικασιών έργων και συστημάτων πληροφορικής. Η παρουσίαση, εκτός από τη βιβλιογραφική αξία της, γίνεται α) για να δειχθούν οι πηγές της φιλοσοφίας και των τεχνικών που εφαρμόζουμε, καθότι σημαντικά στοιχεία τους αποτέλεσαν τη βάση της πρότασής μας, β) για να οριοθετηθεί το πεδίο εφαρμογής της μεθοδολογίας μας, γ) επειδή οι ελλείψεις και η αναποτελεσματικότητα των τεχνικών μεθοδολογιών στο πεδίο των έργων ΗΔ αποτέλεσαν το κίνητρο για την ανάπτυξη της προτεινόμενης μεθοδολογίας, αλλά και για να εξάγουμε συμπεράσματα για το πώς θα έπρεπε να τροποποιηθούν/επεκταθούν αυτές, προκειμένου να καλύψουν την προσέγγιση των πλαισίων ΔΤΠ και δ) για να υποστηριχθεί η εμπιστοσύνη μας στην αποτελεσματικότητα της μεθοδολογίας που προτείνουμε.

Στο τρίτο κεφάλαιο της διατριβής, παρουσιάζεται αναλυτικά η προτεινόμενη μεθοδολογία. Περιγράφεται η δομή της, με τα επίπεδα και τις περιοχές κινδύνου που καλύπτει, οι διαστάσεις αξιολόγησης, το βασικό εργαλείο-μήτρα που χρησιμοποιεί για την αξιολόγηση, οι δείκτες με τους οποίους εξάγονται τα αποτελέσματα, ο τρόπος υπολογισμού τους και η ερμηνεία τους, καθώς και η διαδικασία εφαρμογής της μεθοδολογίας. Συνεχίζοντας, η μεθοδολογία επεκτείνεται εισάγοντας την έννοια της αλληλεξάρτησης κινδύνων εντός του ιδίου έργου στον υπολογισμό των πιθανοτήτων, αλλά και μεταξύ έργων που εκτελούνται παράλληλα.

Στο τέταρτο κεφάλαιο της διατριβής η προτεινόμενη μεθοδολογία δοκιμάζεται σε δύο περιπτώσεις εφαρμογής ΑΔ, μία στην ΥΔΚ-ΣΥΖΕΥΞΙΣ και μία σε πρότυπη ΥΔΚ που αναπτύχθηκε στο πλαίσιο της διατριβής αυτής με σκοπό την προστασία προσωπικών δεδομένων και τη διασφάλιση της ελευθερίας βούλησης των ατόμων. Για να τοποθετηθεί στο περιβάλλον της, πρώτα παρουσιάζονται εν συντομία οι δύο ΥΔΚ και μετά γίνεται η εφαρμογή. Στο πρώτο τμήμα του κεφαλαίου παρουσιάζεται το ευρύτερο έργο ΣΥΖΕΥΞΙΣ, στην πρώτη και στη δεύτερή του υλοποίηση και αναλύεται η ΥΔΚ που αποτέλεσε το υποέργο 9. Στη συνέχεια, εφαρμόζεται η προτεινόμενη μεθοδολογία ΑΔ στο τμήμα του έργου που αφορά τους κινδύνους τελικού χρήστη. Στο δεύτερο τμήμα του κεφαλαίου, παρουσιάζεται η πρότυπη ΥΔΚ και μετά εφαρμόζεται η μεθοδολογία

στο τμήμα του έργου που αφορά την πολιτική ηγεσία. Τέλος εξάγονται συμπεράσματα από την δοκιμασία της προτεινόμενης μεθοδολογίας και στις δύο περιπτώσεις εφαρμογής.

Στο πέμπτο κεφάλαιο της διατριβής γίνεται συζήτηση για την αποτελεσματικότητα της προτεινόμενης μεθοδολογίας, της καινοτομίας της προσέγγισης που εισάγει, των κρισίμων παραγόντων για την επιτυχή εφαρμογή της και την εξαγωγή ορθών αποτελεσμάτων, καθώς και των αδυναμιών της. Τέλος προτείνεται αντικείμενο περαιτέρω έρευνας και ανάπτυξής της.

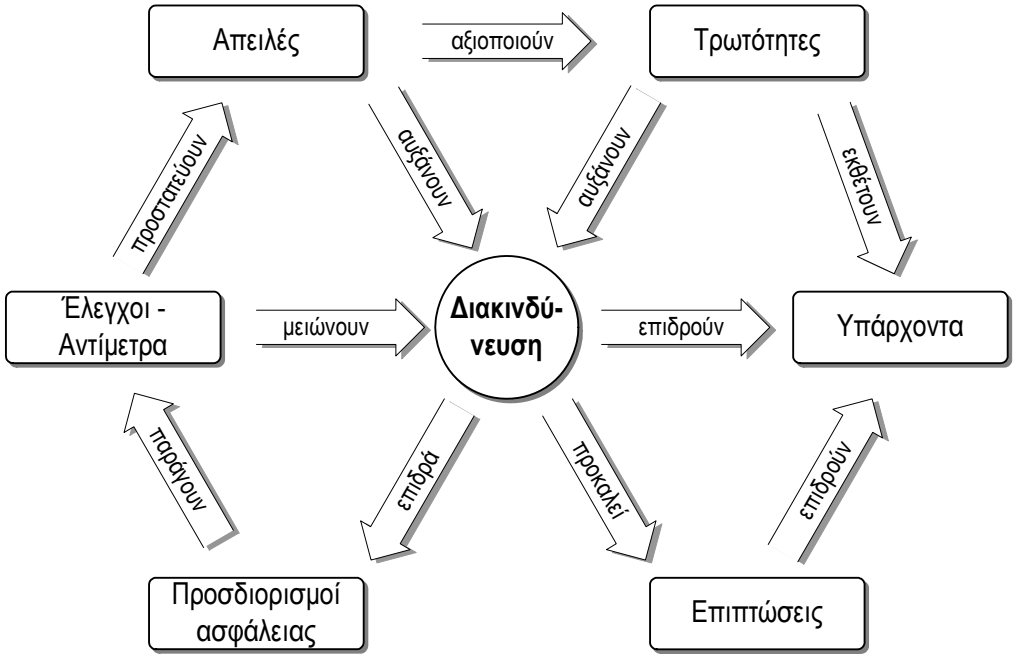
Το Παράρτημα Α περιλαμβάνει πίνακες με το υλικό που συνοδεύει το εργαλείο ΑΔ, το οποίο παρέχει στους αξιολογητές ότι χρειάζεται για την επιτυχή εφαρμογή του και την εξαγωγή χρησίμων αποτελεσμάτων. Το υλικό αυτό είναι προαιρετικό και δεκτικό σε επιλογή, διαμόρφωση και επέκταση από τους αξιολογητές. Περιλαμβάνει επίσης ένα πίνακα με τους συμβολισμούς που χρησιμοποιούνται στις διαδικασίες της πρωτότυπης ΥΔΚ, η οποία χρησιμοποιείται ως περίπτωση εφαρμογής της προτεινόμενης μεθοδολογίας ΑΔ.

1.2 Ορισμός της αξιολόγησης διακινδύνευσης

Η ΑΔ (ή Εκτίμηση Κινδύνου - οι δύο όροι χρησιμοποιούνται εναλλακτικά) μπορεί να οριστεί ως η συστηματική διαδικασία για την ανάλυση, προσδιορισμό, έλεγχο και αναφορά των απειλών (threats) σε ένα σύστημα, έργο ή οργανισμό, της εκτίμησης της πιθανότητας να συμβούν, των τρωτοτήτων (vulnerabilities) στις οποίες επιδρούν και των επιπτώσεών τους όταν συμβούν. Η διακινδύνευση (risk) ορίζεται ως η πιθανότητα τρώσης του συστήματος ή του οργανισμού από τις αναμενόμενες απειλές. Ο συνδυασμός των επιπτώσεων (impacts), των απειλών και των αδυναμιών (weaknesses) των οποίων μπορεί να γίνει εκμετάλλευση, προσδιορίζει το επίπεδο διακινδύνευσης (risk level), το οποίο αποτιμάται συνολικά με το βαθμό διακινδύνευσης (risk grade).

Η ΑΔ πρέπει να κορυφώνεται με τον ορισμό αντιμέτρων (countermeasures) προς μετρίαση (mitigation) των κινδύνων και πρέπει να αποτελεί αναπόσπαστο τμήμα της σχεδίασης και της υλοποίησης οποιουδήποτε συστήματος, το οποίο αποτελεί σημαντικό κτήμα για ένα οργανισμό. Τοιουτοτρόπως, καθιστά δυνατές εμπεριστατωμένες και τεκμηριωμένες αποφάσεις αποτελεσματικής κατανομής κατάλληλων πόρων για την προστασία των σημείων που διατρέχουν τον μεγαλύτερο κίνδυνο, των οποίων η τρώση θα προκαλέσει τη μεγαλύτερη επίπτωση στο σύστημα.

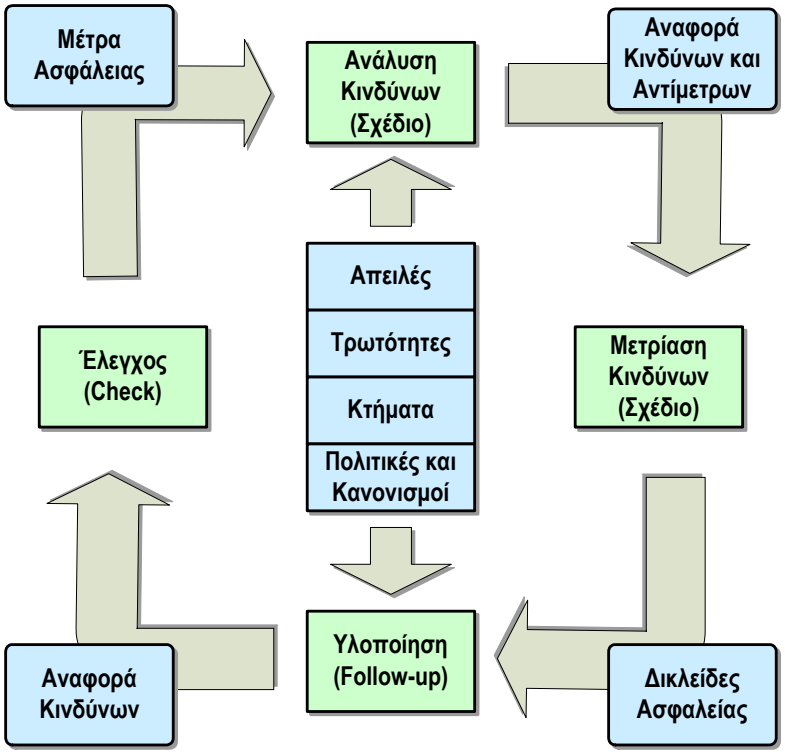
Η ΑΔ αποτελεί ένα μόνο υποστοιχείο (σημαντικό όμως) εντός μιας ευρύτερης πλειάδας διαχειριστικών-διοικητικών δραστηριοτήτων, όπως η εγκαθίδρυση κεντρικής διοίκησης, η εφαρμογή κατάλληλων λειτουργικών πολιτικών, πολιτικών ασφάλειας και αντίστοιχων ελέγχων, η προώθηση επίγνωσης και ενημερότητας ως προς αυτά, καθώς και πολιτικών παρακολούθησης και αξιολόγησης των ελέγχων. Οι σχέσεις ανάμεσα στους κινδύνους, τις απειλές, τις τρωτότητες, τα υπάρχοντα (assets), τις συνέπειες/επιπτώσεις (consequences/impacts) και τον καθορισμό μέτρων και ελέγχων ασφάλειας παρουσιάζονται στο Σχήμα 1 (Gritzalis & Katsikas, 2004).



Σχήμα 1. *Σχέσεις αξιολόγησης διακινδύνευσης*

Η ΑΔ βασίζεται στη θεωρεία στατιστικής λήψης αποφάσεων (statistical decision theory) (Anand, 1993; Hansson, 1994), η οποία, αποδεχόμενη το ενδεχόμενο ότι οποιαδήποτε πληροφορία μπορεί να είναι ανακριβής, χρησιμοποιεί ένα βασικό θεώρημα της θεωρίας πιθανοτήτων, το θεώρημα Bayes, προκειμένου να εκτιμήσει την πιθανότητα για την πραγμάτωση ενός κινδύνου. Στην πράξη, η ΑΔ (της οποίας η εκτίμηση τρωτοτήτων αποτελεί μία μόνο, αλλά σημαντική, φάση) χρησιμοποιείται ευρέως για να υποστηρίξει τη διαδικασία λήψης αποφάσεων, τόσο στον ιδιωτικό, όσο και στο δημόσιο τομέα. Η χρήση τυπικών μεθοδολογιών και εργαλείων ΑΔ για την υποστήριξη της λήψης αποφάσεων γύρω από την ασφάλεια και τη σχετική τεχνολογία, βοηθά στη συνεκτική και αποτελεσματική χρήση των δεδομένων, όπως και στην αφαίρεση της τεχνικής χροιάς από διαδικασίες που είναι κατ' ουσία διοικητικές. Επιπλέον, η ΑΔ πρέπει να εί-

ναι μια επαναληπτική και αυτοελεγχόμενη διαδικασία, όπως φαίνεται στο Σχήμα 2, όπου απεικονίζεται ο κύκλος της διαδικασίας ΑΔ και η θέση, εντός αυτής, των στοιχείων που περιλαμβάνει.



Σχήμα 2. *Κύκλος διαδικασίας αξιολόγησης διακινδύνευσης*

Ειδικότερα, όσον αφορά τις διακριτές φάσεις μιας διαδικασίας ΑΔ, έχουν γίνει πολλές προτάσεις. Το Software Engineering Institute προσδιόρισε τέσσερεις φάσεις (αναγνώριση, ανάλυση, ανάπτυξη απόκρισης, ανάπτυξη ελέγχων) (Tseng et al., 2003), όπως και το Project Management Institute (αναγνώριση, ποσοτικοποίηση, ανάπτυξη απόκρισης και ελέγχων) (Durofee et al., 1996). Οι Klein και Cork (1998) περιέγραψαν μια διαφοροποιημένη διαδικασία τεσσάρων σταδίων (αναγνώριση, ανάλυση, έλεγχος και αναφορά). Ο Boehm (1991) πρότεινε ξεχωριστές φάσεις ΑΔ (αναγνώριση, ανάλυση και ιεράρχηση) και ελέγχου κινδύνων (σχεδίαση διαχείρισης, σχεδίαση πραγμάτωσης και παρακολούθησης, σχεδίαση ιχνηλάτησης και διόρθωσης). Επιπρόσθετα, ο Chapman (1998) πρότεινε εννέα φάσεις (ορισμός, στρατηγική προσέγγιση, καθορισμός κινδύνων, δόμηση πληροφοριών, ιδιοκτησία, εκτίμηση αβεβαιότητας, μέγεθος κινδύνων, απόκριση, παρακολούθηση και έλεγχος). Ο Fairley (1994) θεώρησε επτά φάσεις (καθορισμός, εκτίμηση, μετρίαση, παρακολούθηση, σχεδιασμός έκτακτης ανάγκης, διαχείριση κινδύνων και ανάκαμψη από την κρίση). Κατά το Πρότυπο Διαχείρισης Κινδύνων Αυστρα-

λίας και Ν. Ζηλανδίας, η ΑΔ αποτελείται από οκτώ επαναληπτικές φάσεις: καθορισμός του πλαισίου, αναγνώριση των κινδύνων, ανάλυση των κινδύνων, αξιολόγηση των κινδύνων, αντιμετώπιση των κινδύνων, επικοινωνία και αναφορά, διαβούλευση, παρακολούθηση και επαναξιολόγηση (AS/NZ Standard 4360, 1999). Παρόμοια με τα παραπάνω είναι η μεθοδολογία *Riskman*, που περιγράφει ένα αναλυτικό πλαίσιο εκτίμησης και ελέγχου κινδύνων (Carter et al., 2001).

Συνοψίζοντας, οι μεθοδολογίες ΑΔ περιλαμβάνουν τυπικά τα ακόλουθα στοιχεία:

α) Ανάλυση της σύνθεσης του συστήματος και του περιβάλλοντος στο οποίο καλείται αυτό να λειτουργήσει.

β) Αναγνώριση των απειλών που θα μπορούσαν να βλάψουν και να προκαλέσουν αρνητικές επιπτώσεις στις κρίσιμες λειτουργίες και δομοστοιχεία του. Οι απειλές μπορεί να περιλαμβάνουν εισβολείς, κακοποιούς, δυσαρεστημένους υπάλληλους, τρομοκράτες, φυσικές καταστροφές, αλλά και κακούς χειρισμούς λόγω ανεπαρκούς εκπαίδευσης.

γ) Εκτίμηση της πιθανότητας ότι τέτοιες απειλές θα λάβουν χώρα, βασιζόμενοι σε ιστορικά δεδομένα, στην έρευνα, σε πειράματα, σε προσομοιώσεις, καθώς και στην κρίση και την εμπειρία των εμπειρογνωμόνων.

δ) Καθορισμός και κατηγοριοποίηση της αξίας, της ευαισθησίας και της κρισιμότητας των λειτουργιών, των υπαρχόντων, των περιεχομένων και των διαδικασιών που μπορεί να επηρεαστούν από την πραγμάτωση μιας απειλής, προκειμένου να εκτιμηθεί ποιες/ποια είναι τα πιο σημαντικά.

ε) Εκτίμηση, για τις πιο κρίσιμες και ευαίσθητες λειτουργίες και υποστοιχεία, των δυνητικών απωλειών ή ζημιών που θα προκληθούν, σε περίπτωση υλοποίησης κάθε απειλής, συμπεριλαμβανομένου του κόστους ανάκαμψης του υποστοιχείου και του συστήματος στο σύνολο.

στ) Περιγραφή και δικαιολόγηση αποτελεσματικών και οικονομικά βιώσιμων μέτρων για την εξάλειψη ή τουλάχιστον τη μείωση των κινδύνων, καθώς και την εξασφάλιση ή τουλάχιστον την υποβοήθηση της επιχειρηματικής συνέχειας (business continuity). Εκτός από φυσικά και τεχνολογικά μέτρα, μπορεί να καθορίζονται και νέες διαδικασίες, πολιτικές και δομές οργάνωσης.

ζ) Καταγραφή και επικοινωνία των αποτελεσμάτων της διαδικασίας ΑΔ, εκπόνηση σχεδίου δράσης και πολιτικής επανάληψης της εφαρμογής της.

ΚΕΦΑΛΑΙΟ 2

Υπόβαθρο

Η σελίδα αυτή είναι σκόπιμα λευκή

Σε αυτό το κεφάλαιο της διατριβής, παρατίθενται γνωστές μεθοδολογίες γενικής ΑΔ που χρησιμοποιούνται σε πλήθος τομέων της βιομηχανικής παραγωγής, καθώς και μεθοδολογιών για πληροφοριακά συστήματα και ηλεκτρονικές υπηρεσίες. Συνεχίζοντας, παρουσιάζονται γνωστά πλαίσια ΔΤΠ και το τι έχουν να προσφέρουν, τόσο στην οργάνωση, όσο και στην ανάλυση της ασφάλειας των διαδικασιών έργων και συστημάτων πληροφορικής. Η παρουσίαση, εκτός από την βιβλιογραφική αξία, γίνεται α) για να δειχθούν οι πηγές της φιλοσοφίας και των τεχνικών που εφαρμόζουμε, καθότι σημαντικά στοιχεία τους αποτέλεσαν τη βάση της πρότασής μας, β) για να οριοθετηθεί το πεδίο εφαρμογής της μεθοδολογίας μας, γ) επειδή οι ελλείψεις και η αναποτελεσματικότητα των τεχνικών μεθοδολογιών στο πεδίο των έργων ΗΔ αποτέλεσαν το κίνητρο για την ανάπτυξη της προτεινόμενης μεθοδολογίας, αλλά και για να εξάγουμε συμπεράσματα για το πώς θα έπρεπε να τροποποιηθούν/επεκταθούν αυτές, προκειμένου να καλύψουν την προσέγγιση των πλαισίων ΔΤΠ και δ) για να υποστηριχθεί η εμπιστοσύνη μας στην αποτελεσματικότητα της μεθοδολογίας που προτείνουμε.

2.1 Μεθοδολογίες γενικής αξιολόγησης διακινδύνευσης

Στο κεφάλαιο αυτό θα γίνει ανασκόπηση των σημαντικότερων μεθοδολογιών ΑΔ. Παρατίθενται οι σημαντικότερες μεθοδολογίες γενικής ΑΔ, οι οποίες έχουν χρησιμοποιηθεί για πολλά χρόνια στη βιομηχανική παραγωγή, στον χρηματοπιστωτικό τομέα, στην ασφαλιστική αγορά κα. Γίνεται επίσης ανασκόπηση των σημαντικότερων τεχνικών μεθοδολογιών για πληροφοριακά συστήματα. Τέλος παρουσιάζονται τα πιο γνωστά πλαίσια ΔΤΠ.

Η παρουσίαση, εκτός από την βιβλιογραφική αξία, γίνεται α) για να δειχθούν οι πηγές της φιλοσοφίας και των τεχνικών που εφαρμόζουμε, καθότι σημαντικά στοιχεία τους αποτέλεσαν τη βάση της πρότασής μας, β) για να οριοθετηθεί το πεδίο εφαρμογής της μεθοδολογίας μας, γ) επειδή οι ελλείψεις και η αναποτελεσματικότητα των τεχνικών μεθοδολογιών στο πεδίο των έργων ΗΔ αποτέλεσαν το κίνητρο για την ανάπτυξη της προτεινόμενης μεθοδολογίας, αλλά και για να εξάγουμε συμπεράσματα για το πώς θα έπρεπε να τροποποιηθούν/επεκταθούν αυτές, προκειμένου να καλύψουν την προσέγγιση των πλαισίων ΔΤΠ και δ) για να υποστηριχθεί η εμπιστοσύνη μας στην αποτελεσματικότητα της μεθοδολογίας που προτείνουμε.

Υπάρχουν πολλές μεθοδολογίες για τη διενέργεια ΑΔ και μπορούν να ομαδοποιηθούν σε ποιοτικές (qualitative), βασισμένων σε δέντρα (tree-based) και δυναμικών συστημάτων (dynamic systems).

α) Ποιοτικές μεθοδολογίες

1) Προκαταρκτική αξιολόγηση διακινδύνευσης ή ανάλυση εμποδίων (Preliminary Risk Analysis or Hazard Analysis – PHA). Είναι μια ποιοτική τεχνική που περιλαμβάνει πειθαρχημένη ανάλυση των διαδικασιών γεγονότων που μπορεί να μετατρέψουν ένα πιθανό κίνδυνο σε ένα ατύχημα (Andrews & Moss, 1993). Σε αυτή την τεχνική, πρώτα αναγνωρίζονται πιθανά ανεπιθύμητα γεγονότα και μετά αναλύονται ξεχωριστά. Για κάθε ένα από αυτά στη συνέχεια διατυπώνονται δυνατές βελτιώσεις ή μέτρα πρόληψης. Το αποτέλεσμα αυτής της μεθοδολογίας δείχνει σε ποιες κατηγορίες κινδύνων πρέπει να δοθεί περισσότερη προσοχή και με τη βοήθεια διαγράμματος συχνότητας–αποτελέσματος, οι κίνδυνοι μπορούν να αξιολογηθούν ανάλογα με τη σημαντικότητά τους προκειμένου να δοθεί προτεραιότητα στα αντίστοιχα αντίμετρα.
2) Κίνδυνοι και λειτουργικότητα (Hazard and Operability – HAZOP) (Sutton, 1992), η οποία εξετάζει συστηματικά διαδικασίες και κατασκευαστικές προθέσεις νέων και υπαρχόντων συστημάτων για να εκτιμήσει πιθανούς κινδύνους που οφείλονται σε αποκλίσεις από τα σχεδιαστικά χαρακτηριστικά, καθώς και επακόλουθα παρεπόμενα από αυτούς.
3) Ανάλυση αστοχίας και αποτελεσμάτων (Failure Mode and Effect Analysis – FMEA) (Stamatis, 1995), που εξετάζει κάθε πιθανή αστοχία σε ένα σύστημα προκειμένου να καθορίσει τον τρόπο που το επηρεάζει και να την κατηγοριοποιήσει ανάλογα με την σοβαρότητά της. Όταν η FMEA επεκταθεί με ανάλυση κρισιμότητας (criticality analysis), ονομάζεται ανάλυση αστοχίας και κρισιμότητας αποτελεσμάτων (Failure Mode and Effects Criticality Analysis – FMECA) (Bouti & Kadi, 1994). Παράλληλα οι Price et al. (1992) πρότειναν την αυτοματοποίηση της FMEA με χρήση γνωσιακής βάσης (knowledge base) και οι Bell et al. (1992) τη χρήση μοντέλου αιτιατού λογισμού (causal reasoning model). Επιπλέον οι Kara-Zaitri et al. (1991; 1992) παρουσίασαν βελτιωμένη FMEA που χρησιμοποιεί ολιστική μήτρα (holistic matrix) για να μοντελοποιήσει το σύστημα και σύνολο δεικτών προερχόμενων από πιθανοτικό συνδυασμό (probabilistic combination), προκειμένου να αντικατοπτρίσουν τη σημαντικότητα κάθε συμβάντος σε σχέση με κάθε υποσύνολο, αλλά και με ολόκληρο το σύστημα. Πα-

ρόμοια προσπάθεια έγινε και από τους Pelaez και Bowles (1995) για τη μοντελοποίηση συστήματος με χρήση συγκεχυμένου γνωσιακού χάρτη (fuzzy cognitive map).

β) Μεθοδολογίες βασισμένες σε δέντρα/γράφους

1) Ανάλυση δέντρου σφάλματος (Fault Tree Analysis – FTA), που κατασκευάζει ένα λογικό διάγραμμα, το οποίο δείχνει τις σχέσεις μεταξύ ανεπιθύμητων καταστάσεων και αστοχιών των στοιχείων του συστήματος (Aven, 1992), εντοπίζοντας τις αιτιώδεις σχέσεις των αστοχιών με τη μορφή δενδροειδούς γράφου, με χρήση συμπερασματικής λογικής (deductive logic). Αρχικά ορίζεται ένα ανεπιθύμητο συμβάν ως η ρίζα του δέντρου και στη συνέχεια προσδιορίζονται οι λογικές σχέσεις των αστοχιών που μπορούν να οδηγήσουν σε αυτό το συμβάν ως φύλλα του δέντρου. Το δέντρο σφάλματος μπορεί να χρησιμοποιηθεί σε αξιολόγηση διακινδύνευσης τόσο ποιοτικού, όσο και ποσοτικού τύπου. Η διαφορά είναι ότι το ποιοτικό δέντρο σφάλματος είναι πιο χαλαρό και δεν απαιτεί τόσο αυστηρή δομή όσο το φορμαλιστικό ποσοτικό.
2) Ανάλυση δέντρου γεγονότων (Event Tree Analysis – ETA) (Pate-Cornell, 1984), η οποία χρησιμοποιεί επαγωγική λογική για να παρουσιάσει την ακολουθία των συμβάντων που μπορεί να προκύψουν από ένα επιλεγμένο αρχικό. Χρησιμοποιείται κυρίως για ανάλυση συνεπειών προ ή μετά από ένα συμβάν. Η αριστερή μεριά του δέντρου παρουσιάζει το συμβάν εκκίνησης, η δεξιά την κατάσταση αστοχίας, η επάνω ορίζει τα συστήματα και οι κόμβοι ορίζουν πιθανότητες διακλάδωσης που προκύπτουν από την ανάλυση του συστήματος. Αν το μονοπάτι πηγαίνει προς τα πάνω στον κόμβο, τότε το σύστημα λειτουργεί, αν πηγαίνει προς τα κάτω τότε αποτυγχάνει.
3) Ανάλυση αιτίας-αιτιατού (Cause-Consequence Analysis – CCA), η οποία συνδυάζει ανάλυση αιτίας (δέντρα αστοχιών) και ανάλυση αποτελέσματος (δέντρα συμβάντων), προκειμένου να καθορίσει ακολουθίες συμβάντων που μπορούν να οδηγήσουν σε πιθανά ανεπιθύμητα αποτελέσματα (Aven, 1992). Χρησιμοποιώντας τις πιθανότητες των διαφόρων συμβάντων στο διάγραμμα CCA, υπολογίζονται οι πιθανότητες των παρεπόμενων και έτσι προκύπτει το συνολικό επίπεδο διακινδύνευσης του συστήματος.
4) Αξιολόγηση διακινδύνευσης δέντρου παραλήψεων διοίκησης (Management Oversight Risk Tree – MORT) (Knox & Eicher, 1992). Είναι μια διαγραμματική

μέθοδος που τοποθετεί λογικά τα στοιχεία ασφάλειας και τα αναλύει σε ένα δέντρο σφάλματος, όπου το συμβάν ρίζας είναι το 'Damage, destruction, other costs, lost production or reduced credibility of the enterprise'. Το δέντρο δίνει μια εικόνα για τις αιτίες του συμβάντος ρίζας, είτε από παραλείψεις της διοίκησης, είτε από πιθανούς κινδύνους είτε και από τα δύο. Ένα δέντρο MORT έχει πάνω από 1500 πιθανά βασικά συμβάντα και 100 γενικά συμβάντα.

5) Τεχνική θεώρησης οργάνωσης διαχείρισης ασφάλειας (Safety Management Organization Review Technique – SMORT) (Jouko & Rouhiainen, 1993). Αποτελεί απλοποιημένη έκδοση του MORT και υλοποιείται με χρήση δομημένων επιπέδων ανάλυσης με αντίστοιχους πίνακες ελέγχου, αντί για αναλυτική δομή δέντρου. Η πληροφορία μπορεί να συλλεχθεί με συνεντεύξεις, μελέτη εγγράφων, καθώς και επιτόπου εξέταση. Χρησιμοποιείται για να γίνει ανάλυση ατυχημάτων που έγιναν ή μόλις αποφεύχθηκαν, όπως και έλεγχους και σχεδιασμό ασφάλειας.

γ) *Μεθοδολογίες δυναμικών συστημάτων*

1) Μέθοδος GO (Siu, 1994). Είναι μια τεχνική ανάλυσης στόχου-επιτυχίας, η οποία χρησιμοποιεί δεκαεπτά τελεστές. Κατασκευάζεται ένα μοντέλο του συστήματος από τεχνικά διαγράμματα που αναπαριστούν τα στοιχεία του με τελεστές GO, τριών τύπων – ανεξάρτητους, εξαρτημένους και λογικούς. Οι ανεξάρτητοι τελεστές αναπαριστούν στοιχεία που δεν απαιτούν είσοδο δεδομένων, οι εξαρτημένοι στοιχεία που έχουν τουλάχιστον μία είσοδο και οι λογικοί τελεστές συνδυάζουν τους υπόλοιπους στη λογική επιτυχούς λειτουργίας του συστήματος. Γνωρίζοντας της πιθανότητες των εξαρτημένων και των ανεξάρτητων τελεστών μπορεί να υπολογιστεί η πιθανότητα καλής λειτουργίας του συστήματος.

2) Ανάλυση γραφήματος σφάλματος – πίνακα digraph κατευθυνόμενων γράφων (digraph matrix/fault graph analysis). Χρησιμοποιεί γράφους που αποτελούνται από στοιχεία συστήματος, πύλες AND/OR και βρόχους. Κατασκευάζονται πίνακες ομόριας (adjacency) και συνδεσιμότητας (connectivity), οι οποίοι αναλύονται για να εκτιμηθούν τα μονοπάτια, η προσιτότητα (accessibility), τα singletons (μοναδιαία στοιχεία που μπορεί να προκαλέσουν αστοχία συστήματος) και τα doubletons (ζεύγη στοιχείων που μπορεί να προκαλέσουν αστοχία συστήματος). Οι κατευθυνόμενοι γράφοι (digraph) επιτρέπουν κύκλους και βρόχους ανάδρασης που την κάνουν ελκυστική για ανάλυση δυναμικών συστημάτων.

3) Μοντελοποίηση Markov. Είναι μια κλασική μέθοδος για την εκτίμηση της διαχρονικής συμπεριφοράς δυναμικών συστημάτων. Χρήση μοντέλων Markov έχει γίνει σε πολλά προβλήματα ΑΔ (Pate-Cornell, 1993; Siu, 1994).
4) Μεθοδολογία δυναμικής αναλυτικής λογικής συμβάντων (Dynamic Event Logic Analytical Methodology – DYLAM) (Cojazzi & Cacciabue, 1994). Είναι ένα ολοκληρωμένο πλαίσιο που συνεκτιμά χρόνο, μεταβλητές διαδικασιών και συμπεριφορά συστήματος. Μια DYLAM αποτελείται συνήθως από μοντελοποίηση των στοιχείων του συστήματος, αλγόριθμους υπολογισμού εξισώσεων συστήματος, τοποθέτηση συνθηκών κορυφής, παραγωγή ακολουθιών συμβάντων και ανάλυση αυτών.
5) Μέθοδος ανάλυσης δυναμικού δέντρου συμβάντων (Dynamic Event Tree Analysis – DETAM) (Acosta & Siu, 1993). Υλοποιεί δυναμικό δέντρο συμβάντων, στο οποίο επιτρέπεται η διακλάδωση σε πολλαπλά σημεία στο χρόνο και αφορά χρονική εξέλιξη καταστάσεων υλικού, μεταβλητές διαδικασιών και καταστάσεις χειριστών κατά τη διάρκεια ενός σεναρίου. Χρησιμοποιεί επίσης συλλογή διακλαδωτήρων, συλλογή μεταβλητών συστήματος, κανόνες διακλάδωσης, κανόνες επέκτασης ακολουθιών και εργαλεία ποσοτικοποίησης.

Αυτές οι μεθοδολογίες ΑΔ έχουν χρησιμοποιηθεί για την εκτίμηση του κινδύνου εκτενώς και σε ευρεία γκάμα έργων και εφαρμογών, όπως η παραγωγή ενέργειας, η εξόρυξη πετρελαίου, η κατασκευή ημιαγωγών, η βιομηχανία χημικών, οι οικονομικές αγορές και άλλα.

2.2 Μεθοδολογίες Αξιολόγησης Διακινδύνευσης Πληροφοριακών Συστημάτων και Ηλεκτρονικών Υπηρεσιών

Η ασφάλεια ενός πολύπλοκου συστήματος ΤΠΕ βασίζεται στην ακριβή περιγραφή των στόχων, τη συνεκτική και ολοκληρωμένη μετατροπή τους σε πολιτικές ασφαλείας και την κατάλληλη ανάπτυξη, επιβολή και παρακολούθηση αυτών των πολιτικών. Αυτό πρέπει να ακολουθείται από μια αδιάλειπτη διαδικασία προσαρμογής των πολιτικών σε περιβάλλοντα, τεχνολογίες, χρήση και επιθέσεις που αλλάζουν και εξελίσσονται. Προκειμένου να γίνουν κατανοητές οι πολύπλοκες διασυνδέσεις πολιτικών ασφαλείας, υποδομών, συστημάτων και τρωτοτήτων, για να επικυρωθούν οι στόχοι ασφαλείας, αλλά ιδιαιτέρως για να αυξηθεί το επίπεδο εμπιστοσύνης προς το σύστημα που εξετάζεται,

απαιτούνται τυπικές μεθοδολογίες ΑΔ, βασισμένες σε εργαλεία ανάλυσης. Αυτές μπορούν να καθοδηγήσουν στη διενέργεια συστηματικής εξέτασης και να βοηθήσουν τους επικεφαλείς να αποφασίσουν τι ακριβώς χρειάζεται προστασία και ποιες πολιτικές και μέτρα ασφαλείας πρέπει να εφαρμοστούν.

Εκτός λοιπόν από τις μεθοδολογίες γενικής ΑΔ που αναφέρθηκαν παραπάνω, υπάρχει αριθμός μεθοδολογιών που έχουν αναπτυχθεί ειδικά για την ασφάλεια ΤΠΕ συστημάτων και δικτύων, αποτέλεσμα της έρευνας στον τομέα αυτό. Οι περισσότερες βασίζονται σε συμβολική ερμηνεία που στηρίζεται σε μοντέλα, προσομοίωση και ανάλυση με χρήση γράφων ή δέντρων και μονοπατιών επιθέσεων ή απειλών. Αυτοί είναι αποτελεσματικοί τρόποι για να αντιμετωπιστεί η πολυπλοκότητα, να προβλεφθεί με σχετική ακρίβεια και να αναλυθεί η συμπεριφορά πολυ-διασυνδεδεμένων συστημάτων (τα οποία συχνά διαθέτουν δυναμικά χαρακτηριστικά), έτσι ώστε να ανταποκριθούν σε λειτουργικές απαιτήσεις, στην τεχνολογική εξέλιξη και σε πολυποίκιλα εχθρικά περιβάλλοντα.

Οι Philips και Swiler (1998) ήταν από τους πρωτοπόρους στο θέμα, εισάγοντας ένα μοντέλο βασισμένο σε γράφους, προκειμένου να γίνει αξιολόγηση προσβλητότητας δικτύων. Η μέθοδος βασίζεται σε βάση δεδομένων των συνήθων επιθέσεων αναλυμένων σε ατομικά βήματα, σε περιγραφή της συγκεκριμένης τοπολογίας δικτύου και στη δημιουργία κατατομής του επιτιθέμενου. Γίνεται συνταίριασμα της πληροφορίας επίθεσης, με τη διαμόρφωση του δικτύου και της κατατομής του επιτιθεμένου προκειμένου να παραχθεί γράφος επίθεσης – υπερσύνολο. Οι κόμβοι του αναπαριστούν τη σκηνή της επίθεσης, πχ. τα μηχανήματα στα οποία έχει αποκτήσει πρόσβαση ο επιτιθέμενος και το επίπεδο πρόσβασης στο οποίο έχει αναρριχηθεί. Τα τόξα αναπαριστούν επιθέσεις. Τοποθετώντας πιθανότητες επιτυχίας στα τόξα και κόστη που αναπαριστούν την προσπάθεια που πρέπει να καταβάλει ο επιτιθέμενος, υπολογίζονται τα μονοπάτια επίθεσης με τη μεγαλύτερη πιθανότητα επιτυχίας της επίθεσης, με αλγόριθμους όπως ο συντομότερου δρόμου (shortest path).

Οι Swiler et al. (2001) πρόσθεσαν ένα εργαλείο αυτοματοποιημένης παραγωγής γράφων επίθεσης, που παράγονται αλγοριθμικά από δεδομένα περιγραφής του συστήματος. Το εργαλείο κατασκευάζει τους γράφους με εμπρόσθια εξερεύνηση, ξεκινώντας από μια αρχική κατάσταση. Επιπλέον, ένας συμβολικός ελεγκτής (symbolic checker) κινείται από την κατάσταση-στόχο προς τα πίσω, για να κατασκευάσει τα μονοπάτια επίθεσης, παρακάμπτοντας έτσι τρωτότητες που δεν σχετίζονται με το στόχο του επιτιθεμένου.

Ωστόσο, όταν εφαρμόζονται σε δίκτυα ακόμα και μεσαίου μεγέθους, οι μέθοδοι αυτές υποφέρουν από δυσχερείς οπτικοποιήσεις και εκθετική έκρηξη της πολυπλοκότητας του προβλήματος. Για να αντιμετωπιστεί αυτό οι Ritchey και Ammann (2001), Jha et al. (2002) και Sheyner et al. (2002) πρότειναν τη χρήση αλγορίθμων έλεγχου μοντέλων (model checking) όπως οι SMV και NuSMV, καθώς και παραλλαγές αυτών για τη σύνδεση τρωτοτήτων και την παραγωγή συμπαγών πλήρων γράφων επιθέσεων. Οι Ammann et al. (2002) πρότειναν μια άλλη προσέγγιση με χρήση εμφανούς υπόθεσης μονοτονικότητας (explicit assumption of monotonicity), σύμφωνα με την οποία η προϋπόθεση μιας δεδομένης τρωτότητας δεν ακυρώνεται από την επιτυχή χρήση μιας άλλης, ελαττώνοντας με αυτό τον τρόπο την πολυπλοκότητα του προβλήματος ανάλυσης από εκθετική σε πολυωνυμική.

Από την άλλη μεριά, οι Noel και Jajodia (2004) και ο Rieke (2004) προσπάθησαν να αντιμετωπίσουν την πολυπλοκότητα των γράφων επιθέσεων μέσω ιεραρχικής αναπαράστασης και αφαιρετικών μεθόδων, έτσι ώστε να κάνουν τις οπτικοποιήσεις πιο συμπαγείς και να συμπεριλάβουν ανάλυση ζωτικότητας. Μετέπειτα εξέλιξη (Ou et al., 2006) περιλαμβάνει λογικούς γράφους επιθέσεων, οι οποίοι παρουσιάζουν άμεσα τις λογικές εξαρτήσεις ανάμεσα στους στόχους επίθεσης και την πληροφορία διαμόρφωσης συστημάτων.

Μελλοντικές ερευνητικές εξελίξεις θα μπορούσαν να οδηγήσουν στην ενσωμάτωση εργαλείων ΑΔ στην αυτοματοποιημένη βασισμένη σε πολιτικές αντίδραση σε απειλές (policy-based automated threat response), κάνοντας και χρήση πληροφορίας αναφορών-συναγερμών. Τέτοια συστήματα θα μπορούσαν να βελτιώσουν σημαντικά τα τρέχοντα συστήματα αναγνώρισης και αναχαίτισης διεισδύσεων (intrusion detection and prevention), με συνδυασμό γνώσης της κατάστασης του συστήματος και της ΑΔ, έτσι ώστε να λαμβάνονται καλύτερες αποφάσεις ανταπόκρισης σε συμβάντα, μειώνοντας τα εσφαλμένα-θετικά (false-positives), καθώς και την ενασχόληση των διαχειριστών.

Ωστόσο, ενώ επιστημονικά άρτιες, οι μεθοδολογίες που αναφέρθηκαν απαιτούν προχωρημένη εξειδίκευση, είναι συνήθως δύσκολες στην εφαρμογή τους, δεν περιλαμβάνουν την πιστοποίηση ποιότητας και αξιοπιστίας καθιερωμένων μεθοδολογιών και δεν είναι υποχρεωτικά σύμφωνες με διεθνή πρότυπα ασφάλειας και βέλτιστων πρακτικών. Για το σκοπό αυτό έχουν δημιουργηθεί μεθοδολογίες και πρότυπα, από ιδιωτικούς, κρατικούς και διεθνείς οργανισμούς, οι οποίες έχουν εξελιχθεί σε ολοκληρωμένα εργαλεία, που βοηθούν (στην πραγματικότητα οδηγούν) τους εμπειρογνώμονες και το προ-

σωπικό ασφαλείας στη διενέργεια αποτελεσματικής φορμαλιστικής ΑΔ. Ακόλουθα παρουσιάζουμε εν συντομία τα κυριότερα από αυτά.

CRAMM

Η μεθοδολογία Central Computing and Telecommunications Agency (CCTA) Risk Analysis and Method Management (http://www.insight.co.uk/products/cramm.htm) ήταν αρχικά δημιουργία της κεντρικής υπηρεσίας Data Processing and Telecommunications της κυβέρνησης του Ηνωμένου Βασιλείου (UK). Το αντίστοιχο εργαλείο CRAMM, αυτή τη στιγμή στην 5η του έκδοση, έχει αναπτυχθεί από την βιομηχανία σε συνεργασία με το ανωτέρω γραφείο και την CESG (η αρχή εθνικής ασφάλειας του HB). Ως βιβλιοθήκη ασφάλειας πληροφοριακών συστημάτων, το CRAMM περιλαμβάνει:

α) Εκτενή εργαλεία ΑΔ, συμπεριλαμβανομένων μοντελοποίησης αλληλεξάρτησης υπαρχόντων, εκτίμησης επιχειρηματικής επίπτωσης και συνέχειας, αναγνώρισης και αξιολόγησης απειλών και τρωτοτήτων, αποτίμησης επίπεδου κινδύνου, κατάδειξης και δικαιολόγησης μέτρων.
β) Εργαλείο μοντελοποίησης αλληλεξάρτησης διαδικασιών.
γ) Εργαλεία για την υποβοήθηση διοικητών ασφάλειας πληροφοριών για την σχεδίαση και τη διαχείριση ασφάλειας.
δ) Οδηγούς για την ταχεία κατασκευή φορμαλιστικών πολιτικών ασφάλειας και υποβοηθητική βιβλιογραφία.
ε) Εργαλεία για την υποστήριξη βασικών διαδικασιών στη διαχείριση επιχειρηματικής συνέχειας.
στ) Βάση δεδομένων με πάνω από 3000 ελέγχους και μέτρα ασφάλειας, κατηγοριοποιημένων σε αντίστοιχους κινδύνους και βαθμονομημένων ανάλογα με την αποτελεσματικότητα και το κόστος.

Στο κέντρο του CRAMM βρίσκεται μια βηματική και πειθαρχημένη διαδικασία που περιλαμβάνει και τεχνικές (υλικό και λογισμικό ΤΠΕ συστημάτων) και μη τεχνικές (φυσικές και ανθρώπινες) όψεις ασφάλειας. Προκειμένου να εκτιμήσει αυτά τα στοιχεία, η CRAMM χωρίζεται σε τρεις κύριες φάσεις: α) αναγνώριση στοιχείων και εκτίμηση αξίας τους, β) εκτίμηση απειλών και τρωτοτήτων και γ) επιλογή και πρόταση αντίμετρων.

Στην πρώτη φάση, η CRAMM βοηθά τον ερευνητή να αναγνωρίσει το υλικό, το λογισμικό, τα δεδομένα και τα φυσικά συστατικά που απαρτίζουν το υπό εξέταση σύστη-

μα. Καθένα από αυτά μπορεί να εκτιμηθεί όσον αφορά την αξία του, τα υλικά (με βάση το κόστος αντικατάστασης), το λογισμικό και τα δεδομένα (με βάση την επίπτωση που θα υπήρχε στη περίπτωση μη διαθεσιμότητας, καταστροφής, αποκάλυψης ή τροποποίησης της πληροφορίας).

Έχοντας γίνει κατανοητή η έκταση των δυνητικών προβλημάτων, η επόμενη φάση ενέχει την εκτίμηση της πιθανότητας για να λάβουν χώρα. Η CRAMM καλύπτει πλήρες εύρος σκόπιμων και τυχαίων απειλών, που μπορεί να επιδράσουν σε συστήματα ΤΠΕ, συμπεριλαμβανομένων hacking, κακόβουλων προγραμμάτων, αστοχία υλικού και λογισμικού, σκόπιμη ζημιά, τρομοκρατικές ενέργειες και λάθη από ανθρώπινο παράγοντα. Η φάση αυτή ολοκληρώνεται με τον υπολογισμό του επίπεδου του υποκείμενου ή επικείμενου κινδύνου.

Για την τρίτη φάση, την επιλογή και πρόταση αντιμέτρων, η CRAMM περιλαμβάνει εκτενή βιβλιοθήκη δομημένη σε ιεραρχίες, την οποία απαρτίζουν άνω των 3000 αντιμέτρων, με αναλυτική περιγραφή καθενός, οργανωμένα σε πάνω από 70 λογικές ομάδες. Το λογισμικό χρησιμοποιεί τα μεγέθη των κινδύνων που υπολογίστηκαν στην προηγούμενη φάση προκειμένου να τα συγκρίνει με το επίπεδο ασφάλειας, ένα μέτρο κατωφλίου που σχετίζεται με κάθε αντίμετρο, προκειμένου να καθοριστεί αν οι κίνδυνοι είναι αρκετά σημαντικοί για να δικαιολογείται η εγκατάσταση του συγκεκριμένου αντίμετρου.

Η CRAMM παρέχει τέλος μια σειρά από υποβοηθητικές λειτουργίες, συμπεριλαμβανομένων υπαναχώρηση (backtracking), προετοιμασία απροόπτων (contingency planning), συναρτήσεις ιεράρχησης «τι-εάν» (what-if) και εργαλεία δημιουργίας αναφορών για την υλοποίηση των αντιμέτρων και την ενεργό διαχείριση των αναγνωρισμένων κινδύνων.

COBRA

Το Consultative, Objective and Bi-functional Risk Analysis (http://www.riskworld.net/) είναι ένα εμπορικό εργαλείο ΑΔ, διαβούλευσης και επισκόπησης. Αναπτύχθηκε από ιδιωτικό οργανισμό ώστε να ανταποκριθεί στις απαιτήσεις που ζητούνταν από επιχειρήσεις και οργανισμούς σε αυτούς τους τομείς και ως υποβοήθηση στην πιστοποίηση κατά ISO/IEC 27002/27001. Το COBRA προσπαθεί να κατευθύνει τον εμπειρογνώμονα ασφάλειας προς μια φορμαλιστική μεθοδολογία ΑΔ, έτσι ώστε να εξασφαλίζεται ότι τα μέτρα ασφαλείας που θα ληφθούν είναι ισόμετρα με τους κινδύνους.

Τα κύρια συνθετικά του COBRA είναι: α) ο Σύμβουλος Κινδύνων (ΣΚ – Risk Consultant – RC), β) η διαδικασία ΑΔ, γ) ο Διαχειριστής Δομοστοιχείων (Module Manager – ΜΜ), δ) οι βάσεις γνώσης ΑΔ και ε) ο σύμβουλος ασφαλείας ISO (ISO SC). Ο COBRA RC παρέχει πλήρη υπηρεσία ΑΔ, συμβατή με τις περισσότερες αναγνωρισμένες μεθοδολογίες (ποιοτικές και ποσοτικές), βασισμένη σε ερωτηματολόγια και χρησιμοποιεί αρχές έμπειρων συστημάτων και εκτενή γνωσιακή βάση. Αξιολογεί τη σχετική σημαντικότητα όλων των απειλών και τρωτοτήτων και παράγει τις κατάλληλες προτάσεις και λύσεις. Επιπρόσθετα, οι αναφορές που παράγει παρέχουν γραπτή εκτίμηση και σχετικό βαθμό (ή επίπεδο) κινδύνου, για κάθε κατηγορία κινδύνου. Οι κίνδυνοι που αναγνωρίζονται συνδέονται αυτόματα με δυνητικές επιπτώσεις (οικονομικές, απώλειας κτλ) για τον οργανισμό ή την επιχείρηση.

Για τη διαδικασία ΑΔ, το COBRA ορίζει τρία στάδια: α) Κατασκευή Ερωτηματολόγιων (ΚΕ), β) Χαρτογράφηση Κινδύνων (ΧΚ) και γ) Παραγωγή Αναφορών (ΠΑ). Στο στάδιο ΚΕ κατασκευάζεται το κατάλληλο ερωτηματολόγιο κινδύνων για το σύστημα και το περιβάλλον υπό εξέταση. Ξεχωριστά δομοστοιχεία ερωτήσεων επιλέγονται ειδικά από τη γνωσιακή βάση και κάθε ένα αναφέρεται σε μία ειδική περιοχή κινδύνου ή τάξη απειλών (πχ. λογική πρόσβαση, φυσική πρόσβαση, δίκτυα, ανάπτυξη, επιχειρήσεις). Η δημιουργία του ερωτηματολόγιου μπορεί να γίνει χειροκίνητα ή αυτόματα. Στη φάση ΧΚ οδηγείται η διαδικασία συμπλήρωσης του ερωτηματολόγιου, του και τα δομοστοιχεία του συμπληρώνονται ξεχωριστά από το προσωπικό-στόχο και πιθανώς σε διαφορετικούς χρόνους, κάνοντας έτσι δυνατό το χρονοπρογραμματισμό ανάλογα με τη διαθεσιμότητα. Τα δεδομένα συνενώνονται στη φάση ΠΑ, η οποία παράγει τα αποτελέσματα από τα ερωτηματολόγια, διαμορφωμένα σε πολλαπλά επίπεδα, κατάλληλα για ενημέρωση τόσο τεχνικού όσο και μη τεχνικού διοικητικού προσωπικού.

Ο COBRA ΜΜ χρησιμοποιείται για την διαμόρφωση της παρεχόμενης γνωσιακής βάσης, της οποίας όλα τα περιεχόμενα μπορούν να μεταβληθούν, ακόμα και να δημιουργηθούν νέες βάσεις. Μπορούν επίσης να παραχθούν νέα και να αλλαχθούν τα υπάρχοντα δομοστοιχεία ερωτηματολόγιων, με εκτενείς δυνατότητες διακλάδωσης, όπου απαιτείται, καθώς και ανάθεση βαθμών, βαρών και αντίμετρων σε κάθε απάντηση. Επιπλέον μπορεί να γίνει εισαγωγή και διαχείριση απεριόριστου κείμενου υποβοήθησης για τις ερωτήσεις, κάτι πολύ χρήσιμο σε προσεγγίσεις αυτοανάλυσης.

Οι RC και ΜΜ μοιράζονται βιβλιοθήκη εκτίμησης κινδύνων, ειδικών για κάθε περιοχή κινδύνου ή κατηγορία απειλών, η οποία μπορεί να μεταβληθεί και να ειδικευτεί κατά βούληση. Μοιράζονται επίσης βιβλιοθήκη αντιμέτρων και συστάσεων, επίσης

πλήρως διαμορφούμενη. Τα αντίμετρα μπορούν να ομαδοποιηθούν, όπου απαιτούνται πολλαπλές συστάσεις και λύσεις. Όλα τα βάρη και συνδέσεις μεταξύ των στοιχείων της βάσης γνώσης μπορούν να αλλαχθούν, καθώς και τα περιφερειακά δεδομένα, όπως ο διαμορφωτής ερωτηματολόγιων, τα κείμενα κτλ.

Στο COBRA παρέχονται τέσσερεις ξεχωριστές γνωσιακές βάσεις: α) η βάση ασφάλειας πληροφοριακών συστημάτων, β) η βάση επιχειρησιακών κινδύνων, γ) η «γρήγορη» βάση υψηλών κινδύνων και δ) η βάση ηλεκτρονικής ασφάλειας. Οι πρώτες δύο παρέχουν εκτίμηση κινδύνου στον τομέα τους, η τρίτη παρέχει γρήγορη εκτίμηση και επισκόπηση ολόκληρου του επιχειρηματικού συστήματος και η τελευταία απευθύνεται ειδικά σε σύγχρονα δίκτυα υπολογιστών και συστημάτων που βασίζονται σε αυτά.

Ο ISO SC είναι ένα εργαλείο εκτίμησης ασφάλειας ειδικευμένο για εκτιμήσεις απέναντι στο προκαθορισμένο σύνολο βασικών προτύπων και ελέγχων που αποτελούν το πρότυπο ασφάλειας ISO/IEC 27002/27001. Είναι σχεδιασμένος για να λειτουργεί ως οδηγός στη διαδικασία μέτρησης του επιπέδου συμμόρφωσης ενός οργανισμού και να διαμορφώνει κατάλληλες συστάσεις, όπου απαιτείται. Μέσα από σειρά ερωτήσεων πολλαπλών επιλογών ο ISO SC: α) διαμορφώνει το επίπεδο συμμόρφωσης για κάθε μία από τις δέκα κατηγορίες που καλύπτονται από το πρότυπο, β) αναδεικνύει επιπλέον μέτρα που θα πρέπει να εφαρμοστούν για την αύξηση της συμμόρφωσης και τη βελτίωση σαν αποτέλεσμα της ασφάλειας και γ) παράγει περιεκτική αναφορά της διαδικασίας.

EESA

Το End-to-End Security Assessment (Adar, 2002) αφορά την προστασία κρισίμων υποδομών πληροφορικής (Critical Information Infrastructure Protection – CIIP). Αναλύει την «ποιότητα ασφάλειας υπηρεσιών» (“Security Quality of Service” – SQOS), κατά το μονοπάτι των κρισίμων διαδικασιών σε ένα επιχειρησιακό περιβάλλον ή σύστημα και αξιολογεί το πόσο οι μηχανισμοί ασφάλειας κατά μήκος του είναι επαρκείς για την προστασία από πιθανές απειλές. Η ανάλυση καλύπτει τόσο υψηλού επιπέδου στρατηγικά όσο και αναλυτικά τεχνικά θέματα ασφάλειας.

MEHARI

Η Méthode Harmonisée d’Analyse de Risque (http://www.clusif.asso.fr/en/production/mehari/) υλοποιεί ένα φορμαλιστικό μοντέλο ΑΔ, με συναρτησιακή παραμετρική ανάλυση, δομοστοιχειωτή δομή υποσυστημάτων και διαδικασιών, κατηγοριοποίηση υπαρχόντων (assets), ανίχνευση τρωτοτήτων μέσω επιθεώρησης, βέλτιστη επιλογή διορθω-

τικών ενεργειών και μέτρα συμμόρφωσης με το ISO/IEC 27002. Αντικατέστησε προγενέστερο εργαλείο που ονομάζεται MARION το 2007.

OCTAVE

Το Operationally Critical Threat, Asset and Vulnerability Evaluation (http://www.cert.org/octave/), που αναπτύχθηκε από το Ινστιτούτο Ανάπτυξης Λογισμικού του Πανεπιστήμιου Carnegie Mellon, είναι συστηματικός τρόπος προκειμένου ένας οργανισμός να αντιμετωπίσει τους κινδύνους ασφάλειας για τα πληροφοριακά του συστήματα, μοντελοποιώντας τον πολύπλοκο ιστό οργανωτικών και τεχνολογικών στοιχείων. Η προσέγγιση του OCTAVE περιλαμβάνει σύνολο κριτηρίων που ορίζουν τις απαιτήσεις για μια περιεκτική και αυτοκατευθυνόμενη αξιολόγηση κινδύνων πληροφοριών και μια ευρεία γκάμα μεθόδων και μέτρων συνεπών με αυτούς.

Riskwatch

Το RiskWatch για πληροφοριακά συστήματα και το ISO/IEC 27002 (http://www.riskwatch.com/ISRiskWatchProduct.html) είναι ένα εργαλείο για τη διεξαγωγή αυτοματοποιημένης ΑΔ και διερεύνησης τρωτοτήτων. Παρέχει γνωσιακές βάσεις που μπορούν να διαμορφωθούν από το χρήστη, συμπεριλαμβανομένης της δυνατότητας να οριστούν νέες κατηγορίες υπαρχόντων, απειλών, τρωτοτήτων, ασφαλιστικών δικλείδων και ερωτημάτων. Υποστηρίζει επίσης την κατασκευή σεναρίων τι-εάν (what-if) και ανάλυση οικονομικού αντίκτυπου.

2.3 Πλαίσια Διοίκησης Τεχνολογίας της Πληροφορίας

Τα εργαλεία που αναφέρθηκαν παραπάνω έχουν χρησιμοποιηθεί ευρέως για ΑΔ σε μεγάλη γκάμα έργων και συστημάτων ΤΠΕ, στον ιδιωτικό και στον δημόσιο τομέα, καλύπτουν δε ικανοποιητικά τεχνικούς και οργανωτικούς κινδύνους. Ωστόσο, όπως θα αναπτύξουμε στην επόμενη ενότητα, δεν αντιμετωπίζουν ευθέως, ρητά και αναλυτικά σημαντικά θέματα που παρουσιάζονται ειδικά σε έργα ΗΔ, τόσο στο τεχνικό, όσο και στο διοικητικό επίπεδο. Αυτή η προσέγγιση θεωρείται περιοχή της ΔΤΠ, η οποία αντικατοπτρίζει ευρύτερες αρχές διοίκησης, ενώ ταυτόχρονα επικεντρώνεται στη διαχείριση και χρήση της ΤΠΕ, ώστε να επιτευχθούν οι στόχοι απόδοσης του οργανισμού. Επειδή όμως επιτρέπουν τον ορισμό και την προσαρμογή στοιχείων τους (όπως κίνδυνους, τρωτότητες και αντίμετρα), παρέχουν την ευκαιρία και το κίνητρο να τα επεκτείνουμε με το δικό μας ειδικευμένο εργαλείο, χρησιμοποιώντας τις γνωσιακές βάσεις κινδύνων, εκτί-

μησης πιθανοτήτων, επιπτώσεων και αντίμετρων στη δική μας μεθοδολογία, όπου ταιριάζουν.

Από την άλλη μεριά, η ΔΤΠ συμπεριλαμβάνει τις πολιτικές και τις διαδικασίες που απαιτούνται για να διασφαλιστεί ότι τα πληροφοριακά συστήματα ενός οργανισμού υποστηρίζουν τους στόχους του, ότι χρησιμοποιούνται υπεύθυνα και ότι – το πιο σημαντικό – οι κίνδυνοι γι' αυτά και τον οργανισμό ελαχιστοποιούνται. Επιπλέον, η αποτελεσματική ΔΤΠ αποτελεί σημαντικό στοιχείο συμμόρφωσης σε πρότυπα και νομικά πλαίσια, καθότι υπάρχουν πολλοί κανονισμοί και νόμοι που εφαρμόζονται στην πληροφορία που κατέχει ένας οργανισμός, δημόσιος ή ιδιωτικός, το μεγαλύτερο μέρος της οποίας βρίσκεται εντός συστημάτων ΤΠΕ.

Υπάρχουν πολλά ευρέως γνωστά μοντέλα και αντίστοιχα πρότυπα ΔΤΠ (Elieson, 2006), με τα οποία οι οργανισμοί μπορούν να την προσεγγίσουν, προσαρμόζοντας και υιοθετώντας και μέσα σε αυτά η ασφάλεια αποτελεί τον κεντρικό πυρήνα. Τα πρότυπα αποτελούν συνήθως διεθνείς προσπάθειες, διαχειριζόμενες από κυβερνητικούς οργανισμούς και αντιπροσωπεύουν την εμπειρία και τις βέλτιστες πρακτικές μεγάλου αριθμού οργανισμών και σωμάτων.

ISO/IEC 27002

'Code of Practice for Information Security Management' (ISO/IEC, 2005b) είναι το μόνο διαθέσιμο ειδικό για την ασφάλεια διεθνές πρότυπο ΔΤΠ, το οποίο, όντας αρκετά ευρύ στο πεδίο του, μπορεί να εφαρμοστεί σε μεγάλη γκάμα εφαρμογών και οργανισμών, συμπεριλαμβανομένων και έργων ΗΔ. Πολλοί οργανισμοί καταβάλλουν σημαντική προσπάθεια για να πιστοποιηθούν σε αυτό, παράλληλα με άλλα πιο γνωστά πρότυπα οργάνωσης και διοίκησης, όπως το ISO 9001/9002.

Συμπληρωματικά πρότυπα είναι τα 27001 – 'A specification for an Information Security Management System' (ISO/IEC, 2005a), 27003 – 'Information security management system implementation guidance' (ISO/IEC, 2010), 27004 – 'Information security management – measurement' (ISO/IEC, 2009) και 27005 – 'Information security risk management' (ISO/IEC, 2008). Το τελευταίο αξίζει ιδιαίτερης προσοχής, καθώς, ενώ δεν αποτελεί ένα λειτουργικό εργαλείο ΑΔ όπως αυτά που αναφέρθηκαν παραπάνω, παρέχει πολύτιμες κατευθυντήριες γραμμές για τη διαχείριση κινδύνου, υποστηρίζει τα γενικά θέματα που ορίζονται στο 27001 και είναι σχεδιασμένο να υποβοηθά στην αποτελεσματική εφαρμογή ασφάλειας των πληροφοριών. Βασίζεται σε ολιστική προσέγγι-

ση διαχείρισης κινδύνου, ενώ ταυτόχρονα είναι εφαρμόσιμο σε όλους τους τύπους οργανισμών (ιδιωτικών εμπορικών, δημόσιων, μη-κερδοσκοπικών κτλ) που προτίθενται να διαχειριστούν τις απειλές που μπορεί να διακινδυνεύσουν την ασφάλεια των συστημάτων τους.

COBIT

To Control Objectives for Information and related Technology (http://www.isaca.com/cobit/), αυτή τη στιγμή στην 5η του έκδοση, είναι ένα πλαίσιο ΔΤΠ που έχει δημιουργηθεί από την Information Systems Audit and Control Association (ISACA). Στοχεύει στο να παρέχει ξεκάθαρη πολιτική και ποιοτικές πρακτικές προς την καλύτερη αντίληψη και διαχείριση των κινδύνων που ενέχονται και το επιτυγχάνει προσφέροντας ένα φορμαλιστικό πλαίσιο και λεπτομερείς αντικειμενοστραφείς οδηγούς για διοικητές, χειριστές διαδικασιών, χρήστες και ελεγκτές. Οι κατευθυντήριες γραμμές του είναι μεν γενικού τύπου, όμως είναι καλά δομημένες και πιο περιεκτικές, κατάλληλες και υψηλού επιπέδου από τα καθαρά τεχνολογικά πρότυπα, αποτελώντας ένα από τα κύρια προτερήματά του. Σε αυτές συμπεριλαμβάνονται οι ακόλουθες κύριες κατευθύνσεις, κάποιες από τις οποίες έχουμε υιοθετήσει και προσαρμόσει στη δική μας μεθοδολογία ΑΔ:

α) Κρίσιμοι Παράγοντες Επιτυχίας (ΚΠΕ – Critical Success Factors – CSF). Ορίζουν τα πιο σημαντικά θέματα ή πράξεις που θα πρέπει να εξεταστούν ή να επιτευχθούν προκειμένου να υπάρχει έλεγχος και αποτελεσματικότητα στις διαδικασίες, με σκοπό την τελική επιτυχία στο ανειλημμένο εγχείρημα. Είναι κατευθυντήριες γραμμές προς την διοίκηση, που προσδιορίζουν τα σημαντικότερα θέματα που θα πρέπει να αντιμετωπιστούν, στρατηγικά, τεχνικά, οργανωτικά και διαδικαστικά.

β) Βασικοί Δείκτες Στόχων (ΒΔΣ – Key Goal Indicators – KGI). Αποτελούν δείκτες που αναδεικνύουν το αν μια διαδικασία έχει πετύχει τις απαιτήσεις που έχουν τεθεί για αυτήν.

γ) Βασικοί Δείκτες Απόδοσης (ΒΔΑ – Key Performance Indicators – KPI). Είναι μετρικά υποβοήθησης, που χρησιμεύουν στην εκτίμηση του κατά πόσον μια διαδικασία αποδίδει όσον αφορά την επίτευξη των στόχων της. Αποτελούν εμπρόσθιους ενδείκτες για το αν οι στόχοι είναι πιθανό να επιτευχθούν ή όχι, καθώς και μετρητές δυνατοτήτων, πρακτικών και δεξιοτήτων, διαδικασιών, ομάδων και ολόκληρων οργανισμών.

ITIL

Το IT Infrastructure Library (http://www.itil-officialsite.com/) είναι ένα σύνολο εννοιών και τεχνικών για τη διαχείριση υποδομών ΤΠΕ. Στην τρέχουσα έκδοσή του, το ITILv3 ακολουθεί μια «προσέγγιση ζωής» στην καθοδήγηση της ΔΤΠ, σε αντίθεση με την οργάνωση κατά την καθαρά τεχνολογική οδό. Αποτελείται από σύνολο κειμένων κορμού, τα οποία υποστηρίζονται από συμπληρωματικό υλικό σε μορφή ιστοσελίδας, που ορίζουν βέλτιστες τεχνικές σε 24 τομείς. Η τρέχουσα «βιβλιοθήκη» αποτελείται από τα βιβλία: α) στρατηγικής υπηρεσιών, β) σχεδίασης υπηρεσιών, γ) μετάπτωσης υπηρεσιών, δ) λειτουργία υπηρεσιών και ε) αέναης βελτίωσης υπηρεσιών. Το ITIL στοχεύει κυρίως στο να αναδείξει τις βέλτιστες πρακτικές για τη διοίκηση και διαχείριση των επιπέδων υπηρεσιών ΤΠΕ.

2.4 Συμπεράσματα ανασκόπησης υπόβαθρου

Από την παραπάνω ανασκόπηση των προτύπων ΔΤΠ συμπεραίνουμε ότι, ενώ το COBIT δίνει έμφαση σε ελέγχους και μετρικά απόδοσης συστημάτων ΤΠΕ, το ISO/IEC 27002 επικεντρώνεται στην ασφάλεια συστημάτων ΤΠΕ, ενώ το ITIL εστιάζει σε διαδικασίες και υπηρεσίες. Και ενώ τα παραπάνω πρότυπα αποτελούν πολύ καλά μοντέλα ΔΤΠ και ασφάλειας ΤΠΕ, καλύπτοντας οργανωτικά, διαδικαστικά και πρακτικά θέματα πολύ καλά, στην πράξη βρίσκουμε ότι έχουν μικρή συσχέτιση με τις τεχνικές μεθοδολογίες και εργαλεία ΑΔ, αν εξαιρέσει κανείς ότι προτείνουν (τουλάχιστον στην περίπτωση του ISO/IEC 27002) τη χρήση μιας από αυτές στη φάση σχεδίασης ενός έργου.

Από την άλλη μεριά, παρόλο που κάποια από τα εργαλεία τεχνικής ΑΔ διαθέτουν ειδικά δομοστοιχεία για να βοηθήσουν στην επίτευξη συμμόρφωσης με το ISO/IEC 27002, θεωρούμε ότι θα έπρεπε να υπάρχει μια πιο καλά ορισμένη και συστηματική διεπαφή μεταξύ ΔΤΠ και ΑΔ και ότι η τεχνική ΑΔ θα έπρεπε να διευρύνει το πεδίο της προκειμένου να καλύψει θέματα διοικητικά/διαχειριστικά, υιοθετώντας περισσότερα στοιχεία από τη φιλοσοφία του COBIT. Πιο σημαντικά, πιστεύουμε ότι τα εργαλεία τεχνικής ΑΔ δεν καλύπτουν σημαντικές περιοχές και σημεία κινδύνου που σχετίζονται με έργα ΗΔ, περιοχές και σημεία που αποτελούν μεγαλύτερες απειλές για την επιτυχή ολοκλήρωση, την επίτευξη των στόχων και την ορθή και αποτελεσματική λειτουργία τους, απ' ότι οι συνηθισμένες απειλές προς την ασφάλεια. Αυτό έχει δείξει μακρόχρονη εμπειρία, συμμετοχή και παρατήρηση έργων ΗΔ, όπου πολλά έργα με πολύ θετικές αρ-

χικές προοπτικές και στόχους, τελικά υπολειτούργησαν, έπεσαν σε αχρηστία ή ακόμα και δεν έφτασαν ποτέ σε παραγωγική λειτουργία, λόγω μη πρόβλεψης και μη αντιμετώπισης μη τεχνικών κινδύνων, από το ευρύτερο πολιτικό, διοικητικό και κοινωνικό τους περιβάλλον.

Οι δυσκολίες που παρουσιάζονται εντός του θεσμικού πλαισίου και του κανονιστικού περιβάλλοντος που καλούνται να λειτουργήσουν οι οργανισμοί που αναλαμβάνουν προσπάθειες ΗΔ, έχουν γίνει κρίσιμες. Υπό αυτές τις συνθήκες, πρέπει να ληφθούν υπόψη όχι μόνο νόμοι και κανονισμοί, αλλά και νόρμες, ενέργειες, συμπεριφορές και δυνατότητες ευρείας γκάμας ενδιαφερομένων μερών (Lim et al., 2007; Tan et al., 2007). Η επιτυχία των πρωτοβουλιών ΗΔ μπορεί να επηρεαστεί από ατζέντες πολιτικής, ανεπαρκή πολιτική και διοικητική δέσμευση, μη ετοιμότητα, έλλειψη ενημέρωσης και εκπαίδευσης του ευρύτερου κοινού, όπως και πολλούς οικονομικούς και εμπορικούς παράγοντες (Titah & Barki, 2006). Ασαφείς ή αντιφατικοί νόμοι και κανονισμοί, ισορροπίες μεταξύ εκτελεστικών, νομοθετικών και δικαστικών εξουσιών, αρνητικές συνήθειες, συμπεριφορές και προκαταλήψεις, ακόμα και ψυχολογικοί παράγοντες, μπορεί να περιορίσουν τις προσπάθειες και να οδηγήσουν σε αντίσταση στην αλλαγή και εσωτερικές συγκρούσεις. Επιπλέον, λόγω της τεχνικής και διαδικαστικής πολυπλοκότητας που διαθέτουν, των νεοτερισμών που εισάγουν και των εργασιακών πρακτικών που ενέχουν οι τεχνολογίες ΤΠΕ, τόσο στο επίπεδο του τελικού χρήστη, όσο και στο επίπεδο των σχεδιαστών και εργολάβων, είναι βασικό να εξασφαλιστεί η τεχνολογική και διοικητική ικανότητα των βασικών εμπλεκομένων στο έργο.

Η επαναληπτική διαδικασία ανάλυσης, σχεδίασης και λήψης αποφάσεων πρέπει να είναι κεντρική στην προσπάθεια για καλύτερη κατανόηση των κινδύνων που σχετίζονται με θέματα κανονιστικά, διοικητικά, λειτουργικά, οικονομικά, οργανωτικά, προμηθειών και τελικών χρηστών. Επίσης, η συμμετοχή των τελικών χρηστών, του προσωπικού ΤΠΕ και ασφάλειας, όπως και του προσωπικού της δημόσιας διοίκησης, πρέπει να θεωρείται απαραίτητη. Επιπρόσθετα, πρέπει να τονιστεί η σημαντικότητα του έγκαιρου διαλόγου με όλες τις κατηγορίες χρηστών, έτσι ώστε να αντιμετωπιστούν οι έγνοιές τους και να εκτιμηθούν προληπτικά οι κίνδυνοι για το έργο· και βέβαια ο αντίστοιχος σχεδιασμός, προσπάθεια και συντονισμός για την εγκαθίδρυση ευνοϊκής κουλτούρας.

Σε αυτό το περιβάλλον χρειάζονται εργαλεία ΑΔ που να είναι μεστά και περιεκτικά, αλλά πάνω από όλα ειδικά φτιαγμένα, έτσι ώστε να είναι δυνατή η αποτελεσματική και ασφαλής υλοποίηση έργων και εφαρμογών ΗΔ. Σε αυτό το πλαίσιο αναπτύχθηκε η

προτεινόμενη μεθοδολογία, βασιζόμενη στις προαναφερθέντες απαιτήσεις, αλλά και για να επικοινωνήσει τις αντίστοιχες έγνοιες και απόψεις.

Στο επόμενο κεφάλαιο περιγράφουμε λοιπόν μια μεθοδολογία ΑΔ, μαζί με το αντίστοιχο εργαλείο εφαρμογής, τα οποία προτείνουμε ως πιο κατάλληλα στο πεδίο δράσης ενός έργου ΗΔ από τις συμβατικές που προαναφέρθηκαν. Στοχεύουμε στο να καλύψουμε μεγαλύτερη γκάμα απειλών για την αδιάκοπη, αποτελεσματική και ασφαλή υλοποίηση, ολοκλήρωση και λειτουργία ενός έργου ή συστήματος, πέρα από αυτά που καλύπτονται από μια κλασική διαδικασία τεχνικής ΑΔ (όπως τεχνολογία, υποδομές και κακόβουλες ομάδες), απειλές που πηγάζουν από το ευρύτερο περιβάλλον στο οποίο εξελίσσονται έργα ΗΔ. Φιλοδοξούμε να καλύψουμε κρίσιμες διαστάσεις κινδύνου όπως πολιτισμικές κοινωνικές, πολιτικές, οικονομικές και ψυχολογικές, οι οποίες αφορούν διοικητές, υλοποιητές, χειριστές και χρήστες του συστήματος.

Η σελίδα αυτή είναι σκόπιμα λευκή

ΚΕΦΑΛΑΙΟ 3

Η μέθοδος RIPC^4: Αξιολόγηση Διακινδύνευσης για ασφαλή έργα Ηλεκτρονικής Διακυβέρνησης

Η σελίδα αυτή είναι σκόπιμα λευκή

Σε αυτό το κεφάλαιο της διατριβής, παρουσιάζεται αναλυτικά η προτεινόμενη μεθοδολογία. Περιγράφεται η δομή της, με τα επίπεδα και τις περιοχές κινδύνου που καλύπτει, οι διαστάσεις αξιολόγησης, το βασικό εργαλείο-μήτρα που χρησιμοποιεί για την αξιολόγηση, οι δείκτες με τους οποίους εξάγονται τα αποτελέσματα, ο τρόπος υπολογισμού τους και η ερμηνεία τους, καθώς και η διαδικασία εφαρμογής της μεθοδολογίας. Συνεχίζοντας, η μεθοδολογία επεκτείνεται εισάγοντας στον υπολογισμό των πιθανοτήτων την έννοια της αλληλεξάρτησης κινδύνων εντός του ιδίου έργου, αλλά και μεταξύ έργων που εκτελούνται παράλληλα.

3.1 Μεθοδολογία Αξιολόγησης Διακινδύνευσης

3.1.1 Επισκόπηση μεθοδολογίας

Η προτεινόμενη μέθοδος (Kefallinos et al., 2009, 2011) στοχεύει να λειτουργήσει ως εργαλείο ΑΔ, απευθυνόμενο σε μηχανικούς συστημάτων ΤΠΕ, ειδικούς διαχείρισης ασφάλειας και διοικητικά στελέχη με τεχνική κατάρτιση, στις φάσεις προγραμματισμού, σχεδίασης και υλοποίησης ενός έργου/συστήματος, με περιοδικό και επαναληπτικό τρόπο. Έχει οραματιστεί ως ένα ελαφρύ, ταχύ και ποιοτικό δομοστοιχείο, συμπληρωματικό σε καθιερωμένες μεθοδολογίες ΑΔ, προσανατολισμένο στις ειδικές απαιτήσεις έργων ΗΔ και προορισμένο για χρήση με τη μεθοδολογία συλλογής στοιχείων τύπου ειδικών ομάδων-στόχου ή προσωπικών συνεντεύξεων, χωρίς όμως να περιορίζει τους χειριστές του και το πεδίο εφαρμογής του. Εναλλακτικά, θα μπορούσε να χρησιμοποιηθεί σε κυκλική μέθοδο τύπου Delphi (Delbecq et al., 1975; Schmidt et al., 2001), όπου η ομάδα ειδικών αξιολογεί (βασιζόμενοι στις διαστάσεις αξιολόγησης που εισάγει) το επίπεδο κινδύνου του εξεταζόμενου έργου ΗΔ, σε προσπάθεια διαμόρφωσης ομόφωνης εκτίμησης.

Η προτεινόμενη μεθοδολογία περιλαμβάνει ογδόντα εννέα περιοχές κινδύνου (risk areas), ομαδοποιημένες σε έντεκα επίπεδα κινδύνου (risk levels), οι οποίες αξιολογούνται σε επτά σχετικές διαστάσεις αξιολόγησης.

Οι περιοχές και τα επίπεδα έχουν συγκεντρωθεί από εμπειρία πεδίου, αναφορές διεθνών και εθνικών έργων (Durham, 2002; Hampshire, 2006; OECD, 2001; Tasmania, 2005), καθώς και από σχετική βιβλιογραφία (Ebrahim & Irani, 2005; Evangelidis, 2007; Evangelidis et al., 2002; NECCC, 2000; Vassilakis et al., 2005). Η μεθοδολογία συλλογής επικεντρώθηκε στις ιδιαιτερότητες που εισάγονται με την συμμετοχή και αλληλεπί-

δραση πολιτικής ηγεσίας, δημόσιας διοίκησης, αναδόχων/εργολάβων και πολιτών στα έργα. Τα επίπεδα κινδύνου που προτείνονται αξιολογούνται παράλληλα με αυτά που εκτιμούνται τυπικά σε μια διαδικασία τεχνικής ΑΔ, με σκοπό την εκτίμηση του βαθμού του κινδύνου που διατρέχει το έργο από αυτά.

Τα έντεκα επίπεδα κινδύνου είναι τα ακόλουθα:

1) Πολιτικό (political),
2) Διοικητικό (managerial),
3) Προσωπικού υπηρεσίας (service staff),
4) Αναδόχου/εργολάβου (contractor),
5) Τελικού χρήστη (end-user),
6) Κοινωνικό (social),
7) Προϋπαρχόντων λειτουργικών πολιτικών/διαδικασιών (pre-existing operational policies/procedures),
8) Νομικό/κανονιστικό (legal/regulatory),
9) Οικονομικό (financial),
10) Προμηθειών (procurement) και
11) Διαλειτουργικότητας (interoperability).

Οι ογδόντα εννέα περιοχές κινδύνου, αριθμημένες και ομαδοποιημένες στα έντεκα επίπεδα, είναι οι ακόλουθες. Η αρίθμησή τους είναι σημαντική, διότι χρησιμοποιείται στους γράφους αλληλεξάρτησης κινδύνων (βλ. Κεφάλαιο 4). Η έννοια αυτών γίνεται πιο κατανοητή με αναφορά στους αντίστοιχους παρεχόμενους ΚΠΕ και Αντίμετρα (βλ. Πίνακα 1).

Α. Πολιτικό επίπεδο
   1) Υποστηριχτική αποφασιστικότητα και λήψη αποφάσεων
   2) Μεσο/μακρο-πρόθεσμος ενιαίος σχεδιασμός και δέσμευση στο έργο (πολιτικό επίπεδο)
   3) Κοινωνική και εμπορική τοποθέτηση και αιτιολόγηση (πόσο καλά τοποθετείται το έργο για να ανταποκριθεί και να καλύψει κοινωνικές και εμπορικές ανάγκες) από την πολιτική ηγεσία
   4) Υποστήριξη για/από άλλες συμπληρωματικές ή ακολουθιακές πολιτικές και έργα (πολιτικό επίπεδο)
   5) Κουλτούρα τεχνολογίας της πολιτικής ηγεσίας
   6) Εξοικείωση της πολιτικής ηγεσίας με το έργο (σε υψηλό επίπεδο)

7) Επαρκής και διαχρονική κατανομή πιστώσεων (υψηλό στρατηγικό επίπεδο)
8) Κατανομή αρμοδιότητας/δικαιοδοσίας μεταξύ κυβερνητικών υπηρεσιών
9) Τοποθέτηση και αλληλεπίδραση με/εντός εθνικών πολιτικών και βραχυ/μεσο-πρόθεσμων εθνικών στρατηγικών (πολιτικό επίπεδο)
10) Τοποθέτηση και αλληλεπίδραση του έργου με περιφερειακές και κεντρικές διεθνείς οδηγίες, πολιτικές και έργα (πολιτικό επίπεδο)
11) Παρουσίαση, αιτιολόγηση και προώθηση του έργου στο προσωπικό κατώτερου κυβερνητικού/διοικητικού επιπέδου, στα ΜΜΕ και το ευρύ κοινό (πολιτικό επίπεδο)
12) Οικονομικές, διοικητικές και διαπροσωπικές σχέσεις (όπου σχετίζονται και μπορούν να επηρεάσουν το έργο) με τοπικές και εθνικές οικονομικές και παραγωγικές δυνάμεις, εθνικά/τοπικά ΜΜΕ
13) Οικονομικές, διοικητικές και πολιτικές σχέσεις και συνθήκες (που σχετίζονται και μπορούν να επηρεάσουν το έργο) με γειτονικές, περιφερειακές και κεντρικές κυβερνητικές, οικονομικές και παραγωγικές δυνάμεις, διεθνή ΜΜΕ
14) Πρόβλεψη, διασφάλιση και παρακολούθηση αποτελεσματικότητας ως προς την παροχή κινήτρων για την ορθή και υπεύθυνη υλοποίηση, λειτουργία και χρήση του έργου, προς τη διοίκηση, τους αναδόχους/εργολάβους, το προσωπικό υπηρεσίας και το κοινό στο οποίο απευθύνεται (πολιτικό επίπεδο)

Β. Επίπεδο Διοίκησης

15) Βραχυ/μεσο-πρόθεσμος ενιαίος σχεδιασμός και δέσμευση στο έργο (επίπεδο διοίκησης)
16) Επαρκής σχεδίαση και αιτιολόγηση επιχειρηματικής περίπτωσης (business case development)
17) Κατάλληλη και πλήρης σχεδίαση και επίβλεψη της στρατηγικής εκτέλεσης του έργου
18) Λειτουργική, στόχο-προσανατολισμένη, με τεχνολογική επίγνωση και φιλική προς το χρήστη σύνταξη και επίβλεψη χαρακτηριστικών του έργου
19) Τεχνολογική κουλτούρα του διοικητικού προσωπικού
20) Εξοικείωση του διοικητικού προσωπικού με το έργο
21) Νομική, κανονιστική, πολιτική (policy) και διαδικαστική προσαρμογή προς το έργο και συμμόρφωση από το έργο

22) Αρμόζουσα εκχώρηση αρμοδιοτήτων και εξουσίας στην ιεραρχία διακυβέρνησης και διοίκησης
23) Αιτιολόγηση κόστους, ολικά, μερικά και κατά στάδια και δομοστοιχεία
24) Μεθοδολογία διασφάλισης παραγωγικότητας, παρακολούθησης προόδου και απόδοσης ευθύνης
25) Τεχνολογική, διαδικαστική και διοικητική ετοιμότητα εταίρων (εξωτερικών οργανισμών)
26) Υποστήριξη για / από άλλες συμπληρωματικές ή ακολουθιακές πολιτικές και έργα (επίπεδο διοίκησης)
27) Κατανομή προσωπικού, ανάπτυξη και διασφάλιση προσόντων αυτού
28) Παρουσίαση, αιτιολόγηση και προώθηση του έργου στο προσωπικό κατώτερου κυβερνητικού/διοικητικού επιπέδου και το ευρύ κοινό (επίπεδο διοίκησης)
29) Πρόβλεψη, διασφάλιση, παροχή και παρακολούθηση της αποτελεσματικότητας κινήτρων για την ορθή και υπεύθυνη υλοποίηση, λειτουργία και χρήση του έργου, από τους αναδόχους/εργολάβους, το προσωπικό υπηρεσίας και το κοινό στο οποίο απευθύνεται (επίπεδο διοίκησης)
30) Ποιότητα διεπαφής διοίκησης, προσωπικού υπηρεσίας και τελικού χρήστη – σχεδίαση και διασφάλιση καλώς ορισμένων και αποτελεσματικών διαδικασιών, ευκολία πρόσβασης (επίπεδο διοίκησης)
31) Πίστη στα κίνητρα και στους τεθειμένους στόχους της πολιτικής ηγεσίας όσον αφορά το έργο (επίπεδο διοίκησης)

Γ. Επίπεδο προσωπικού υπηρεσίας

32) Εξοικείωση και εκπαίδευση του κατανεμηθέντος προσωπικού
33) Φιλικότητα του συστήματος προς το προσωπικό υπηρεσίας
34) Αρμόζον τεχνικό επίπεδο (μπορεί να επηρεάσει σε μεγάλο βαθμό την απόδοση του προσωπικού υπηρεσίας σε απρόβλεπτες καταστάσεις)
35) Κίνητρα για την σωστή, ασφαλή και αποτελεσματική χρήση του συστήματος
36) Κίνητρα για την ταχεία, αποτελεσματική και ευγενή υποστήριξη των τελικών χρηστών
37) Ανατροπή εξουσιών, αρμοδιοτήτων και ισορροπιών λόγω νέων τεχνολογιών και γνώσης – δημιουργία φραγμών, κλειστών ομάδων και ανταγωνισμού (επίπεδο προσωπικού υπηρεσίας)

38) Αλλαγή καθηκόντων που μπορεί να απαιτηθούν από οργανωτικές και διαδικαστικές μεταβολές, είτε για την υποστήριξη, είτε ως αποτέλεσμα της υλοποίησης του έργου
39) Φόβοι απώλειας εργασίας με την υιοθέτηση νέων τεχνολογικών και διαδικασιών
40) Ικανότητες επικοινωνίας του προσωπικού υπηρεσίας – επηρεάζει σημαντικά την αποτελεσματικότητά του (επίπεδο προσωπικού υπηρεσίας)
41) Ποιότητα διεπαφής προσωπικού υπηρεσίας / τελικού χρήστη – υιοθέτηση καλώς ορισμένων και αποτελεσματικών διαδικασιών, ευκολία πρόσβασης (επίπεδο προσωπικού υπηρεσίας)
42) Πίστη στα κίνητρα και στους τεθειμένους στόχους του συστήματος από την πολιτική ηγεσία και την διοίκηση (επίπεδο προσωπικού υπηρεσίας)

Δ. Επίπεδο Αναδόχου/Εργολάβου

43) Δεξιότητες και τεχνική κατάρτιση προσωπικού
44) Τεχνολογική αρτιότητα και μακροχρόνια επένδυση σε αυτή
45) Παρελθούσα εμπειρία σχετική με το έργο
46) Παρελθούσα εμπειρία με τον φορέα του έργου
47) Δεξιότητες επικοινωνίας (προφορική και γραπτή)
48) Κίνητρα/δεσμεύσεις για σωστή υλοποίηση και υποστήριξη του έργου
49) Ακριβής υλοποίηση της επιχειρηματικής περίπτωσης, σχεδίασης και χαρακτηριστικών
50) Ακριβής και πλήρης τεκμηρίωση διαδικασιών, λεπτομερειών υλοποίησης και παραλλαγοδότησης (versioning)
51) Θετικές προς την έκβαση του έργου σχέσεις με την πολιτική και διοικητική ιεραρχία
52) Πιστοποίηση οργάνωσης, διαδικασιών, τεχνικής κατάρτισης και ασφάλειας, σύμφωνα με διεθνή πρότυπα και ελεγκτικούς μηχανισμούς

Ε. Επίπεδο τελικού χρήστη

53) Εξοικείωση με το έργο
54) Τεχνολογική κουλτούρα
55) Φιλικότητα χρήσης του συστήματος
56) Εμπιστοσύνη προς το σύστημα, ιδιαίτερα όπου υπάρχει θέμα αποθήκευσης και χρήσης προσωπικών/ιδιωτικών δεδομένων

57) Κίνητρα για χρήση (οικονομικά, χρονικά, ανάγκες)
58) Κίνητρα για υπεύθυνη/ασφαλή χρήση
59) Ευκολία πρόσβασης σε απαραίτητα υλικά και υπηρεσίες
60) Κόστος και προαπαιτούμενα υλικών ή/και χρήσης του συστήματος
61) Ποιότητα διεπαφής προσωπικού υπηρεσίας / τελικού χρήστη – ύπαρξη καλώς ορισμένων, αποτελεσματικών διαδικασιών, ευκολία πρόσβασης (επίπεδο τελικού χρήστη)
62) Ικανότητες επικοινωνίας του προσωπικού υπηρεσίας – επηρεάζει σημαντικά την άποψη των χρηστών για το σύστημα (επίπεδο τελικού χρήστη)
63) Ικανοποίηση των προσδοκιών των χρηστών
64) Θέματα πολυγλωσσίας πολυπολιτισμικότητας
65) Πίστη στα κίνητρα και στους τεθειμένους στόχους του συστήματος από την πολιτική ηγεσία (επίπεδο τελικού χρήστη)

ΣΤ. Κοινωνικό επίπεδο

66) Ανατροπή εξουσιών και ισορροπιών λόγω νέων τεχνολογιών και γνώσης – δημιουργία φραγμάτων, κλειστών ομάδων και ανταγωνισμού (κοινωνικό επίπεδο)
67) Διείσδυση σε κλειστές ή απομονωμένες κοινωνικές ομάδες στόχου (πχ. εθνότητες, μειονότητες, φύλο, αγροτικές, νομαδικές)
68) Πίστη στα κίνητρα και στους τεθειμένους στόχους του συστήματος από την πολιτική ηγεσία (κοινωνικό επίπεδο)
69) Θετική ψυχολογία μάζας προς το έργο και ανταπόκρισή του σε κοινωνικές ανάγκες, συνθήκες και κουλτούρα
70) Επαρκής και θετική κάλυψη του έργου από τα ΜΜΕ

Ζ. Επίπεδο προϋπαρχόντων πολιτικών/διαδικασιών

71) Συμβατότητα με υπάρχουσες πολιτικές και διαδικασίες
72) Σχεδιασμός για ταχεία απόκριση σε μη αναμενόμενα θέματα πολιτικών/διαδικασιών

Η. Νομικό/κανονιστικό επίπεδο

73) Εκ των προτέρων μελέτη νομικής/κανονιστικής συμμόρφωσης
74) Νομικός/κανονιστικός εναρμονισμός μεταξύ χωρών
75) Επίσημη και ξεκάθαρη ανάθεση αρμοδιοτήτων
76) Προσαρμογή νομικού/κανονιστικού πλαισίου στις ανάγκες του έργου

77) Ρυθμιστικό πλαίσιο λειτουργίας και εφαρμογή του από προσωπικό υπηρεσίας και χρήστες
78) Τοποθέτηση και αλληλεπίδραση εντός/με εθνικών πολιτικών και βραχυ/μεσο-πρόθεσμων εθνικών στρατηγικών (νομικό/κανονιστικό επίπεδο)
79) Σχεδιασμός για ταχεία απόκριση σε μη αναμενόμενα νομικά και κανονιστικά θέματα

Θ. Οικονομικό επίπεδο

80) Σχεδιασμός και ανάπτυξη επιχειρηματικής περίπτωσης (οικονομικό επίπεδο)
81) Κατάλληλη κατανομή προϋπολογισμού
82) Διαχείριση και παρακολούθηση πιστώσεων/κεφαλαίων

I. Επίπεδο προμηθειών

83) Διαδικασίες έγκαιρων προμηθειών
84) Διαχείριση αποθήκης, εφοδιαστικής αλυσίδας και υλικού

ΙΑ. Επίπεδο διαλειτουργικότητας

85) Χρήση ειδικής εφαρμογής παρακολούθησης και διαχείρισης της ολοκλήρωσης των τεχνολογιών εντός του έργου
86) Ύπαρξη και συμμόρφωση με πρότυπα διαλειτουργικότητας
87) Συμβατότητα προς τα πίσω με υπάρχοντα συστήματα και συμβατότητα προς τα μπρος με σχεδιαζόμενα μελλοντικά συστήματα
88) Σχεδιασμός, παρακολούθηση και έλεγχος μετάπτωσης δεδομένων από συστήματα προς αντικατάσταση
89) Μελέτη και πρόβλεψη συνεργασίας, μεταφοράς/ανταλλαγής δεδομένων, εξαρτήσεων και βηματοδότησης υλοποίησης (implementation pacing) με άλλα έργα

Οι επτά διαστάσεις αξιολόγησης είναι οι ακόλουθες:

1) Επίπτωση του κινδύνου (risk impact) στην αποτελεσματική και ασφαλή ανάπτυξη και λειτουργία του συστήματος,
2) Πιθανότητα να λάβει χώρα ο κίνδυνος (risk probability),
3) Σχετιζόμενοι ΚΠΕ (CSFs),
4) Αντίμετρα (countermeasures) για μετρίαση του κινδύνου,
5) Κόστος Αντιμέτρων (countermeasure cost), ποιοτικό,
6) Κατώφλι Κάλυψης Κινδύνου (risk coverage threshold),

7) Εκτίμηση Κάλυψης Μετρίασης Κινδύνου των αντιμέτρων (countermeasure risk mitigation coverage estimate).

Συνολικά η πρόταση για τα επίπεδα και τις περιοχές κινδύνου που περιλαμβάνει η μεθοδολογία, μαζί με τις σχετικές διαστάσεις αξιολόγησης, παίρνει (για λόγους παρουσίασης) τη μορφή της μήτρας Κίνδυνος-Επίπτωση-Πιθανότητα-ΚΠΕ-Αντίμετρα-Κόστος-Κάλυψη (Risk-Impact-Probability-CSF-Countermeasures-Cost-Coverage – RIPC^4). Σε αυτήν οι διαστάσεις αξιολόγησης έχουν τη μορφή στηλών και οι περιοχές και τα επίπεδα κινδύνου τη μορφή γραμμών. Για λόγους συντομίας στην παρουσίαση, παρατίθενται μόνο λίγες από τις γραμμές (Πίνακας 1).

Οι περισσότερες περιοχές κινδύνου αναφέρονται στη μήτρα ως συνθήκες με εννοούμενο το πρόθεμα «απουσία», ενώ ορισμένες αποτελούν φανερά ευθείες συνθήκες. Μερικές από τις περιοχές κινδύνου παρουσιάζονται σε παραπάνω από ένα επίπεδα, κάτι που οφείλεται στο ότι διαφορετικές γωνίες αντίληψης δημιουργούν διαφορετικό κίνδυνο, ανάλογα με τους ανθρώπους ή την περιοχή που απειλείται. Οι περιοχές κινδύνου που παρατίθενται θα μπορούσαν να αναλυθούν περαιτέρω σε πολλά υποστοιχεία επικινδυνότητας, ωστόσο στον Πίνακα 1 αντιμετωπίζονται ως ένας ενιαίος κίνδυνος, για λόγους συντομίας.

3.1.2 Υπολογισμός διαστάσεων αξιολόγησης

Σαν μέρος του προτεινόμενου εργαλείου εφαρμογής ΑΔ, ακολουθεί ο τρόπος υπολογισμού των επτά κανονιστικών διαστάσεων αξιολόγησης και τα πεδία τιμών τους:

α) Επίπτωση (Impact) – μεταβλητή συνδεδεμένη με τον κίνδυνο. Λαμβάνει τιμές σε δεκαβάθμια αριθμητική κλίμακα και αναπαριστά το αποτύπωμα που θα έχει η πραγμάτωση του κινδύνου-απειλής στην επιτυχία του έργου, με την τιμή 1 να σημαίνει σχεδόν καμία επίπτωση και την τιμή 10 να σημαίνει αποτυχία (μη πραγμάτωση των στόχων) του έργου. Ο υπολογισμός της γίνεται με την εξής διαδικασία:

Πίνακας 1. *Κίνδυνος-Επίπτωση-Πιθανότητα-ΚΠΕ-Αντίμετρα-Κόστος-Κάλυψη (RIPC^4)*

Η βασική μήτρα RIPC^4 με τις ογδόντα εννέα περιοχές κινδύνου σε έντεκα επίπεδα, καθώς και τις επτά διαστάσεις αξιολόγησης.

Α / Α	**Κίνδυνος**	**Επί-πτωση**	**Πιθανό-τητα**	**ΚΠΕ**	**Αντίμετρα**	**Κόστος Αντιμέ-τρων**	**Κατώφλι Κάλυψης**	**Κάλυψη**
Α	***Πολιτικό Επίπεδο***							
1	Υποστηριχτική αποφασιστικότητα και λήψη αποφάσεων							
2	Μεσο/μακρο-πρόθεσμος ενιαίος σχεδιασμός και δέσμευση στο έργο (πολιτικό επίπεδο)							
---	---	---	---	---	---	---	---	---
---	---	---	---	---	---	---	---	---
88	Σχεδιασμός, παρακολούθηση και έλεγχος μετάπτωσης δεδομέ-νων από συστήματα προς αντικατάσταση							
89	Μελέτη και πρόβλεψη συνεργασίας, μεταφοράς/ανταλλαγής δε-δομένων, εξαρτήσεων και βηματοδότησης υλοποίησης (imple-mentation pacing) με άλλα έργα							

Κάθε κίνδυνος αναλύεται καταρχήν σε σύνολο *n* αποτελεσμάτων (effects), τα οποία θα λάβουν χώρα σε περίπτωση πραγμάτωσής του. Κάθε αποτέλεσμα *j* (*j* = 1…*n*), αναπαρίσταται από το άνυσμα [REb_j, REw_j, RE_j], όπου REb_j δυαδική μεταβλητή με τιμή 1 αν το αποτέλεσμα προκαλεί αυτοδύναμα ολική αποτυχία του έργου και 0 αν δεν την προκαλεί, REw_j μεταβλητή βάρους σε δεκαβάθμια αριθμητική κλίμακα (λειτουργεί ως έκφραση της σημαντικότητάς του σε σχέση με τα άλλα αποτελέσματα του κινδύνου) και *REj* το ποσοστό αποτυχίας του έργου, σε εκατονταβάθμια κλίμακα, που προκαλείται από αυτό το αποτέλεσμα. Ο λόγος χρήσης σύνθετης μεταβλητής για τον υπολογισμό της επίπτωσης είναι η επίτευξη ταυτόχρονα απλότητας και ευελιξίας στον τρόπο που αυτή υπολογίζεται. Τελικά, η επίπτωση I_i του κινδύνου *i* δίνεται από τον τύπο:

$$I_i = MAX\left\{ MAX\left\{REb_j\right\}\cdot 10, \frac{\sum_j \left(1 - REb_j\right) REw_j RE_j}{10\sum_j REw_j} \right\} \quad \text{όπου } j = 1\ldots n$$

Προφανώς από τον τύπο, εάν ένα από τα REb_j = 1, τα υπόλοιπα αποτελέσματα δεν λαμβάνονται υπόψη και I_i = 10.

β) Πιθανότητα (probability) – μεταβλητή συνδεδεμένη με τον Κίνδυνο. Παίρνει τιμές σε αριθμητική κλίμακα από μηδέν έως ένα. Αντιπροσωπεύει το ενδεχόμενο να λάβει χώρα η απειλή, να πραγματωθεί ο κίνδυνος. Η εκτίμηση της πιθανότητας γίνεται τυπικά με συστήματα υποστήριξης αποφάσεων (decision support systems), που χρησιμοποιούν είτε αναλυτική διαδικασία ιεραρχίας (Analytical Hierarchy Process – AHP) (Saaty, 2001), είτε Bayesian Belief Networks (BBN) (Press, 1989), είτε ένα από τα εμπορικά εργαλεία ΑΔ, όπως αυτά που αναφέραμε παραπάνω, με επιπλέον υποστήριξη από ιστορικά δεδομένα και προσωπική έρευνα και εμπειρία πεδίου. Σαν μέρος της μεθοδολογίας που περιγράφεται, προτείνεται η ακόλουθη διαδικασία.

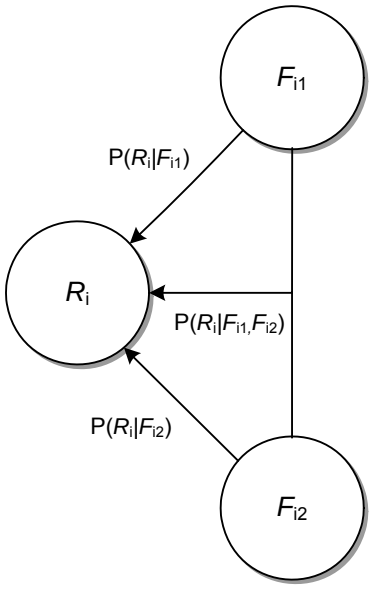
Βήμα 1

Καταγράφονται οι παράγοντες (factors) οι οποίοι μπορεί να προκαλέσουν την πραγμάτωση ενός κινδύνου. Αυτοί μπορεί να βρεθούν με ανάλυση της φύσης του κινδύνου και αντιστοίχιση στο περιβάλλον υλοποίησης και τα χαρακτηριστικά του έργου/συστήματος που ταιριάζουν. Στη συνέχεια κατασκευάζεται ένα BBN σύγκλησης πίστης (converging belief BBN), όπως στο Σχήμα 3 (όπου απεικονίζεται ένα BBN για την εκτίμηση της πιθανότητας πραγμάτωσης ενός

κινδύνου R_i, ο οποίος μπορεί να προκληθεί-επηρεάζεται από δύο παράγοντες, F_{i1} και F_{i2}), των παραγόντων και του κινδύνου με τις υποθέσεις ότι:

α) τόσο ο κίνδυνος, όσο και οι παράγοντες είναι δυαδικές μεταβλητές (δηλ. παίρνουν τιμές ΝΑΙ ή ΟΧΙ, συμβαίνει ή δεν-συμβαίνει) και

β) κάποιοι παράγοντες, όταν λαμβάνουν χώρα, επηρεάζουν την πιθανότητα κάποιων άλλων να συμβούν.



Σχήμα 3. Παράδειγμα BBN ενός κινδύνου και δύο παραγόντων

Η πιθανότητα κάθε παράγοντας να συμβεί εκτιμάται από ανάλυση του περιβάλλοντος και των διαδικασιών του έργου, με ιστορικά στοιχεία, με ερωτηματολόγια και με συνεντεύξεις του προσωπικού που εμπλέκεται. Με βάση αυτά εκτιμάται εύκολα η πιθανότητα του κινδύνου μέσω του BBN και των τύπων εξαρτημένης πιθανότητας. Πχ. για δύο παράγοντες F_{i1} και F_{i2} και ένα κίνδυνο R_i , έστω:

F_{i1}		F_{i2}	
True	False	True	False
$P(F_{i1})=0,1$	$P(F_{i1}')=0,9$	$P(F_{i2})=0,4$	$P(F_{i2}')=0,6$

	F_{i1}	True		False	
	F_{i2}	True	False	True	False
R_i	True	$P(R_i \mid F_{i1}, F_{i2})=0,8$	$P(R_i \mid F_{i1}, F_{i2}')=0,6$	$P(R_i \mid F_{i1}', F_{i2})=0,5$	$P(R_i \mid F_{i1}', F_{i2}')=0,5$
	False	$P(R_i' \mid F_{i1}, F_{i2})=0,2$	$P(R_i' \mid F_{i1}, F_{i2}')=0,4$	$P(R_i' \mid F_{i1}', F_{i2})=0,5$	$P(R_i' \mid F_{i1}', F_{i2}')=0,5$

Τότε:

$$
\begin{aligned}
P(R_i) &= P(R_i, F_{i1}, F_{i2}) + P(R_i, F'_{i1}, F_{i2}) + P(R_i, F_{i1}, F'_{i2}) + P(R_i, F'_{i1}, F'_{i2}) \\
&= P(R_i \mid F_{i1}, F_{i2})\, P(F_{i1}, F_{i2}) + \\
&\quad P(R_i \mid F'_{i1}, F_{i2})\, P(F'_{i1}, F_{i2}) + \\
&\quad P(R_i \mid F_{i1}, F'_{i2})\, P(F_{i1}, F'_{i2}) + \\
&\quad P(R_i \mid F'_{i1}, F'_{i2})\, P(F'_{i1}, F'_{i2}) \\
&= P(R_i \mid F_{i1}, F_{i2})\, P(F_{i1})\, P(F_{i2}) + \\
&\quad P(R_i \mid F'_{i1}, F_{i2})\, P(F'_{i1})\, P(F_{i2}) + \\
&\quad P(R_i \mid F_{i1}, F'_{i2})\, P(F_{i1})\, P(F'_{i2}) + \\
&\quad P(R_i \mid F'_{i1}, F'_{i2})\, P(F'_{i1})\, P(F'_{i2}) \\
&= 0{,}518
\end{aligned}
$$

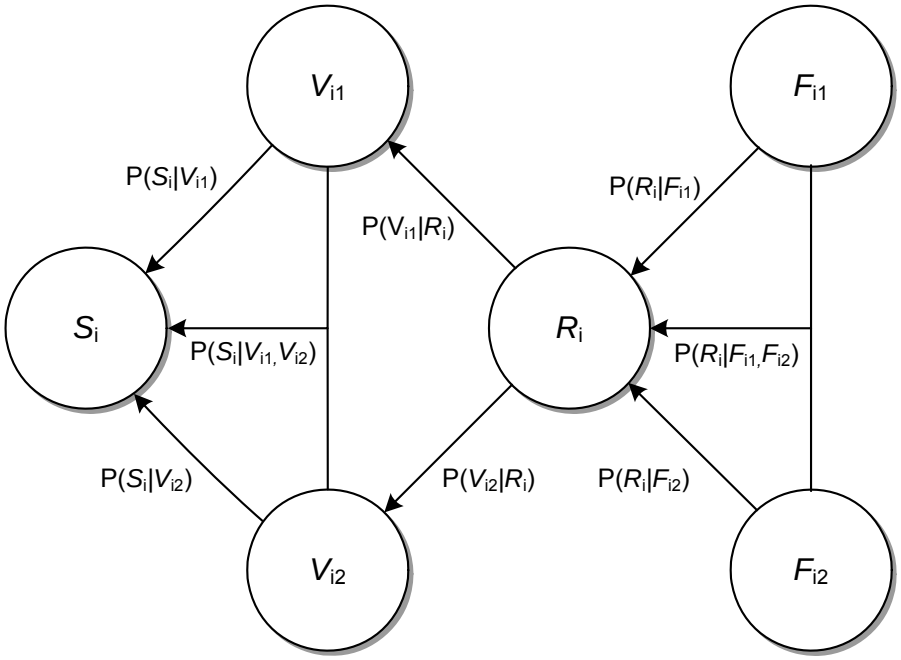
Βήμα 2

Σε αυτό το σημείο οι αξιολογητές θα πρέπει να αποφασίσουν αν θα χρησιμοποιήσουν στη μήτρα RIPC[4] την πιθανότητα που υπολογίστηκε για τον κίνδυνο στο Βήμα 1, ή θα προχωρήσουν στον υπολογισμό της πιθανότητας αστοχίας του συστήματος από αυτόν τον κίνδυνο. Στη δεύτερη περίπτωση, καταγράφονται οι τρωτότητες του έργου/συστήματος, οι οποίες μπορεί να αποτελέσουν στόχο για τον κάθε κίνδυνο (αυτές θα χρησιμοποιηθούν και σε επόμενο στάδιο για τον υπολογισμό της Κάλυψης). Στη συνέχεια, γίνεται η υπόθεση ότι ο κίνδυνος έχει ήδη λάβει χώρα και η πιθανότητα να «ενεργοποιηθεί» καθεμιά από τις τρωτότητες προκαλώντας δυσλειτουργία του συστήματος χρησιμοποιείται για να υπολογιστεί η πιθανότητα ο κίνδυνος να προκαλέσει αστοχία του συστήματος, η οποία θα εισαχθεί στη μήτρα RIPC[4].

Η λογική αυτή δεν μπορεί να εφαρμοστεί τυπικά για κίνδυνους που επιδρούν άμεσα σε δομοστοιχεία τεχνολογικών συστημάτων προκαλώντας αστοχία, εδώ όμως μπορεί να εφαρμοστεί διότι οι κίνδυνοι που εξετάζονται προέρχονται από πηγές όπως το περιβάλλον του συστήματος, οι διαδικασίες που το πλαισιώνουν, οι δομές που το αφορούν (φορείς λειτουργίας, διοίκηση, προσωπικό, χρήστες) κτλ, επιδρώντας έμμεσα στη λειτουργία του ή στην επίτευξη των στόχων του. Ο υπολογισμός της τελικής πιθανότητας για αστοχία του συστήματος από ένα κίνδυνο γίνεται με επέκταση του προηγούμενου BBN ώστε να περιλαμβάνει και τις τρωτότητες, με τελικό κόμβο την αστοχία. Θεωρώντας ότι τόσο οι τρωτότητες, όσο και η αστοχία είναι δυαδικές μεταβλητές, για κάθε τρωτότητα που αφορά

αυτόν τον κίνδυνο, εκτιμάται η πιθανότητα να γίνει εκμετάλλευση της. Εφόσον η εκμετάλλευση αυτής της τρωτότητας επηρεάζει την πιθανότητα εκμετάλλευσης άλλης τρωτότητας, γίνεται συνεκτίμηση αυτής της εξαρτημένης πιθανότητας.

Έχοντας εκτιμήσει τις πιθανότητες όλων των τρωτοτήτων, μέσω του BBN και των τύπων εξαρτημένης πιθανότητας, εκτιμάται η πιθανότητα αστοχίας του συστήματος από αυτό τον κίνδυνο. Το Σχήμα 4 δείχνει ένα ακόμα παράδειγμα με τα νέα δεδομένα, όπου απεικονίζεται ένα BBN για την εκτίμηση της πιθανότητας πραγμάτωσης μιας αστοχίας S_i ενός συστήματος, η οποία προκαλείται από δύο τρωτότητες V_{i1}, V_{i2}, στις οποίες επιδρά ένας κίνδυνος R_i, ο οποίος μπορεί να προκληθεί (επηρεάζεται) από δύο παράγοντες, F_{i1} και F_{i2}.



Σχήμα 4. Παράδειγμα BBN ενός κινδύνου, δύο παραγόντων, δύο τρωτοτήτων

γ) ΚΠΕ – περιγραφικού τύπου σύνθετη μεταβλητή. Οι ΚΠΕ διαφέρουν μεταξύ των περιοχών κινδύνου και των έργων ΗΔ. Στην ουσία συνιστούν ανάλυση της φύσης και της αιτιότητας των κινδύνων που εξετάζονται σε κάθε επίπεδο, καθώς και των παραγόντων που θα πρέπει να εξεταστούν προκειμένου να εκτιμηθεί η επιτυχής υλοποίηση και η επίτευξη των στόχων του έργου. Σαν μέρος του εργαλείου εφαρμογής ΑΔ που συνοδεύει την προτεινόμενη μεθοδολογία αναλύονται στον Πίνακα 2 του Παραρτήματος Α, σύμφωνα με την άποψη του συγγραφέα και τη σχετική βιβλιογραφία, οι πιο σημαντικοί ΚΠΕ, για κάθε έναν από τους κινδύνους.

δ) Αντίμετρα (countermeasures) – περιγραφικού τύπου σύνθετη μεταβλητή. Αποτελείται από κατάλληλα μέτρα που πρέπει να παρθούν, βάσει της φύσης και της δριμύτητας του κινδύνου (επίπτωση – πιθανότητα), καθώς και από τις γνωστές βέλτιστες πρακτικές στο συγκεκριμένο πλαίσιο. Τα τεχνικά αντίμετρα καλύπτονται ικανοποιητικά από τα συνήθη φορμαλιστικά εργαλεία ΑΔ. Τα πολιτικά και κοινωνικά αντίμετρα περιλαμβάνουν εκστρατείες ενημέρωσης, μηχανισμούς προώθησης συναίνεσης, προγράμματα εκπαίδευσης και κατάρτισης και ενδυνάμωση ενδιαφερόμενων μερών. Τέλος, τα οικονομικά αντίμετρα περιλαμβάνουν κίνητρα που διασφαλίζουν την δέσμευση των ενδιαφερομένων, στρατηγικές διαπραγμάτευσης και χρήση σύγχρονων εργαλείων οικονομικής μηχανικής. Σαν μέρος του εργαλείου εφαρμογής ΑΔ που συνοδεύει την προτεινόμενη μεθοδολογία αναλύονται στον Πίνακα 2 του Παραρτήματος Α, σύμφωνα με την άποψη του συγγραφέα και τη σχετική βιβλιογραφία, τα πιο σημαντικά αντίμετρα, για κάθε έναν από τους κινδύνους.

ε) Κόστος Αντιμέτρων (countermeasure cost) – μεταβλητή συνδεδεμένη με τα Αντίμετρα. Επειδή το κόστος δεν μετριέται πάντα με νομισματικούς όρους και μπορεί να περιλαμβάνει άλλους παράγοντες, όπως πιο πολύπλοκη σχεδίαση, καθώς και οργανωτικές και κοινωνικές διαδικασίες, η μεταβλητή αυτή έχει ποιοτική φύση, παίρνοντας τιμές σε δεκαβάθμια αριθμητική κλίμακα, για όλα μαζί τα αντίμετρα κάθε κινδύνου. Ως εκ τούτου, δεν είναι άμεσα αξιοποιήσιμη για να καθοριστεί το πραγματικό κόστος των αντιμέτρων· συμπεριλαμβάνεται εδώ ως ένα μέσο σύγκρισης και επιλογής των πιο αποτελεσματικών, ανάλογα με το κόστος, αντιμέτρων, εκφράζοντας την «πάρε-δώσε» προσέγγιση μεταξύ διαδικασιών που είναι άκαμπτες, αλλά περισσότερο ασφαλείς και διαδικασιών που είναι περισσότερο φιλικές προς το χρήστη, τις λειτουργικές ανάγκες και την ευκολία στη χρήση, αλλά λιγότερο ασφαλείς.

στ) Κατώφλι Κάλυψης (coverage threshold) – μεταβλητή συνδεδεμένη με τον κίνδυνο. Αντιπροσωπεύει την ελάχιστη κάλυψη κίνδυνου, στην οποία εκτιμούν οι σχεδιαστές ότι θα πρέπει να στοχεύουν. Παίρνει τιμές σε δεκαβάθμια αριθμητική κλίμακα και η τιμή της εξαρτάται από την Επίπτωση, την Πιθανότητα και το Κόστος Αντιμέτρων. Όσο υψηλότερη είναι η Επίπτωση του κινδύνου και όσο πιο πιθανός είναι αυτός, τόσο εγγύτερο στην Επίπτωση θα πρέπει να είναι το Κατώφλι. Όσο υψηλότερο είναι το Κόστος Αντιμέτρων, τόσο μπορεί να χαμηλώσει το Κατώφλι, στην οποία περίπτωση μπορεί να θεωρηθεί ως το κατώτερο αποδεκτό όριο της Κάλυψης (βλ. παρακάτω), καθώς και μια πρόβλεψη του περιθωρίου κάλυψης που υπάρχει.

ζ) Εκτίμηση Κάλυψης (coverage estimate) – μεταβλητή συνδεδεμένη με τα αντίμετρα. Παίρνει τιμές σε δεκαβάθμια αριθμητική κλίμακα και αντιπροσωπεύει ένα μέτρο της προστασίας του έργου/συστήματος από τον κίνδυνο μέσω των αντιμέτρων. Η Κάλυψη έχει παρόμοια έννοια με το Κατώφλι, αντιπροσωπεύει όμως το πραγματικό αποτέλεσμα των αντιμέτρων, προς τη μετρίαση του κινδύνου και όχι το επιθυμητό όριο ασφαλείας. Δεν θα πρέπει να είναι χαμηλότερη από το Κατώφλι και θα πρέπει όσο κοντά γίνεται στην Επίπτωση, εκτός και αν οι σχεδιαστές έχουν αποφασίσει να αποδεχτούν ένα ποσό κινδύνου προς μείωση του Κόστους.

Στην περίπτωση πραγμάτωσής του, κάθε κίνδυνος επιδρά πάνω σε ένα ή περισσότερα στοιχεία/χαρακτηριστικά του έργου/συστήματος τα οποία αποτελούν τρωτότητες γι' αυτόν και ως εκ τούτου είναι ειδικές για κάθε έργο/σύστημα. Σαν πρώτο βήμα της διαδικασίας υπολογισμού της Κάλυψης, καταγράφονται οι τρωτότητες του έργου/συστήματος που μπορεί να αποτελέσουν στόχο για τον κάθε κίνδυνο. Γι' αυτές ορίζονται ένα ή περισσότερα αντίμετρα. Ο υπολογισμός της Κάλυψης γίνεται βάσει της επίδρασης που έχουν τα αντίμετρα στην μετρίαση ή εξάλειψη των τρωτοτήτων και ανάλογα με το αν καθένα από αυτά δρα αυτόνομα ή συνδυάζεται (προστίθεται) με την επίδραση άλλου/άλλων.

Εάν λοιπόν C_{ij} είναι το ποσοστό μετρίασης της τρωτότητας i από το αντίμετρο j, για τον κίνδυνο k, (i=1…n, j=1…m, όπου n οι τρωτότητες που έχουν εκτιμηθεί και m τα αντίμετρα που έχουν οριστεί) και I_k η επίπτωση που έχει υπολογιστεί, τότε η συνολική κάλυψη C_k δίνεται από τον τύπο:

$$C_k = I_k \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} C_{ij}}{100n} \quad \text{όπου} \quad \sum_{j=1}^{m} C_{ij} \le 100 \quad \text{για κάθε } i=1\ldots n$$

Σημαντικό σε αυτό τον υπολογισμό είναι να μην γίνει υπερεκτίμηση της επίδρασης των αντιμέτρων στις τρωτότητες και να εκτιμηθεί σωστά ο αριθμός και η φύση των τελευταίων.

Οι πρώτες δύο διαστάσεις αξιολόγησης (Επίπτωση, Πιθανότητα) λειτουργούν στο στην προτεινόμενη μεθοδολογία ως τυπικοί πυλώνες ΑΔ, ενώ οι δύο επόμενες (ΚΠΕ, Αντίμετρα) λειτουργούν ως πυλώνες διαχείρισης κινδύνου. Η συμπερίληψή τους σε φάση μεθοδολογίας ΑΔ στοχεύει στη γρήγορη ποιοτική προ-εκτίμηση των σημαντικών και διαθέσιμων μέτρων, χρησιμοποιούμενες δε σε επαναληπτική βάση, δίνουν επιπλέον

ενόραση των επιπτώσεων των απειλών που εξετάζονται. Οι τελευταίες τρεις διαστάσεις (Κόστος, Κατώφλι, Κάλυψη), παρέχουν ανατροφοδοτούμενο μηχανισμό αυτοελέγχου, προς υποβοήθηση των αξιολογητών για τη σωστή διαμόρφωση των αντιμέτρων και την εξισορρόπηση του Κόστους και της Κάλυψης.

3.1.3 Εξαγωγή αποτελεσμάτων

Στα πλαίσια μιας διαδικασίας ΑΔ, η διεπιστημονική ομάδα ειδικών ασφάλειας, ΗΔ, και ΔΤΠ, θα επιτελέσουν αξιολόγηση τύπου λίστας ελέγχου, με την εξής ακολουθία:

α) Θα επιλέξουν εντός της περιοχής ειδίκευσής τους τα στοιχεία (κίνδυνους) της μήτρας RIPC[4] που αφορούν και εφαρμόζονται στη συγκεκριμένη εφαρμογή ΗΔ, μαζί με τους ΚΠΕ του έργου που σχετίζονται με τον κάθε κίνδυνο.

β) Θα υπολογίσουν τιμές για την Επίπτωση και την Πιθανότητα κάθε κινδύνου, όπως επίσης και την, κατά την κρίση τους, ελάχιστη κάλυψη μετρίασης (Κατώφλι Κάλυψης). Προκειμένου να αξιοποιηθεί πρότερη γνώση και να εκτιμηθούν οι πραγματικές επιπτώσεις και πιθανότητες των στοιχείων κινδύνου, η αξιολόγηση τυπικά γίνεται, όπως αναφέρθηκε παραπάνω, με συστήματα υποστήριξης αποφάσεων που χρησιμοποιούν είτε AHP, είτε BBN, είτε ένα από τα εμπορικά εργαλεία ΑΔ, όπως αυτά που αναφέραμε παραπάνω, με επιπλέον υποστήριξη από ιστορικά δεδομένα και προσωπική εμπειρία πεδίου.

γ) Θα επιλέξουν τα Αντίμετρα που μπορούν να μετριάσουν τον κίνδυνο, προς την πραγματοποίηση των ΚΠΕ.

δ) Για κάθε κίνδυνο θα εισάγουν την εκτίμησή τους για το συνολικό Κόστος των αντιμέτρων που επέλεξαν, με χρήση αντίστοιχων χρηματοπιστωτικών - λογιστικών εργαλείων του οικονομοτεχνικού τομέα.

ε) Τελικά, στην τελευταία στήλη, θα εισάγουν τον υπολογισμό της Κάλυψης μετρίασης του κινδύνου που παρέχεται από τα αντίμετρα που έχουν επιλεγεί για κάθε κίνδυνο, επαναξιολογώντας τα κατά τη διαδικασία. Οι αξιολογητές θα πρέπει να προσπαθήσουν να επιτύχουν Κάλυψη όσο κοντά γίνεται στην τιμή της Επίπτωσης και οπωσδήποτε μεγαλύτερη από το Κατώφλι.

Έχοντας συμπληρώσει τη μήτρα, οι αξιολογητές υπολογίζουν στη συνέχεια τον ΒΔΣ-δείκτη διακινδύνευσης *Ri* και τους ΒΔΑ-δείκτες κάλυψης *Ci*, περιθωρίου κάλυψης *Mi* και συνολικού κόστους *Co* με τους ακόλουθους τύπους:

$$Ri = \frac{\sum_{j=1}^{n} P_j \left(I_j - C_j\right)}{n}, \qquad Ci = \frac{\sum_{j=1}^{n} \left(I_j - \bar{I}\right)\left(C_j - \bar{C}\right)}{\sqrt{\sum_{j=1}^{n} \left(I_j - \bar{I}\right)^2 \sum_{j=1}^{n} \left(C_j - \bar{C}\right)^2}},$$

$$Mi = 1 - \frac{\sum_{j=1}^{n} \left(C_j - \bar{C}\right)\left(Ct_j - \bar{C}t\right)}{\sqrt{\sum_{j=1}^{n} \left(C_j - \bar{C}\right)^2 \sum_{j=1}^{n} \left(Ct_j - \bar{C}t\right)^2}}, \qquad Co = \sum_{j=1}^{n} Co_j$$

$$\bar{I} = \frac{1}{n}\sum_{j=1}^{n} I_j, \qquad \bar{C} = \frac{1}{n}\sum_{j=1}^{n} C_j, \qquad \bar{C}t = \frac{1}{n}\sum_{j=1}^{n} Ct_j$$

όπου n είναι ο συνολικός αριθμών των κινδύνων που αξιολογήθηκαν, P_j είναι η τιμή της Πιθανότητας, I_j η τιμή της Επίπτωσης, C_j η τιμή της Κάλυψης, Ct_j το Κατώφλι Κάλυψης και Co_j το Κόστος των αντιμέτρων, για κάθε κίνδυνο j (όπου $j = 1 \ldots n$).

Αν ο *Ri* είναι κοντά στο 0, τότε μπορεί να θεωρηθεί ότι οι κίνδυνοι έχουν αντιμετωπιστεί (μετριαστεί) επαρκώς, με τις προϋποθέσεις ότι α) έχουν ληφθεί υπόψη όλοι οι παράγοντες κινδύνου (απειλές) και β) έχουν αυτοί καλυφθεί από τα αντίμετρα· δηλαδή ο *Ci* να είναι κοντά στο 1 (ο *Ci* αποτελεί στην πραγματικότητα ένδειξη το πόσο κοντά ακολουθεί η Κάλυψη την Επίπτωση). Όσο υψηλότερος είναι ο *Ri*, τόσο υψηλότερος είναι ο μη-μετριασμένος κίνδυνος. Επιπρόσθετα, ο *Mi* αποτελεί ένδειξη του πόσο κοντά στο όριο (Κατώφλι) είναι η Κάλυψη. Οι αξιολογητές μπορούν να ρυθμίσουν τα αντίμετρα προκειμένου να μειώσουν το συνολικό κόστος *Co* (προφανώς και την κάλυψη), ακόμα αν και αυξηθεί ο *Ri*, όσο ο *Ci* δεν πέφτει πολύ κάτω από το 1 και ο *Mi* δεν πέφτει στο 0.

Σε μια πιο λεπτομερή ανάλυση, θα μπορούσε να δημιουργηθεί ένα γράφημα του *Co* με το *Ri* ή το *Ci*, έτσι ώστε να βρεθεί ο καλύτερος συνδυασμός αντιμέτρων και κόστους, με επαναληπτική υπολογιστική διαδικασία. Κάτι τέτοιο ωστόσο θα ήταν πολύπλοκο και χρονοβόρο, καθώς τα αντίμετρα και η κάλυψη κινδύνου που παρέχουν δεν αποτελούν απλές ρυθμίσιμες μεταβλητές, αλλά σύνθετες ποσότητες, οι οποίες συχνά ενσωματώνουν μακροσκελείς διαδικασίες με αβέβαια αποτελέσματα. Εναλλακτικά, επειδή ο *Ri* έχει άγνωστη κατανομή πιθανότητας, θα μπορούσαν να χρησιμοποιηθούν τεχνικές βέλτιστου ελέγχου στις μεταβλητές *Cj* προκειμένου να προσαρμοστούν, με την προϋπόθεση ότι τα *Ij* θεωρούνται σταθερά για ένα δεδομένο σύστημα.

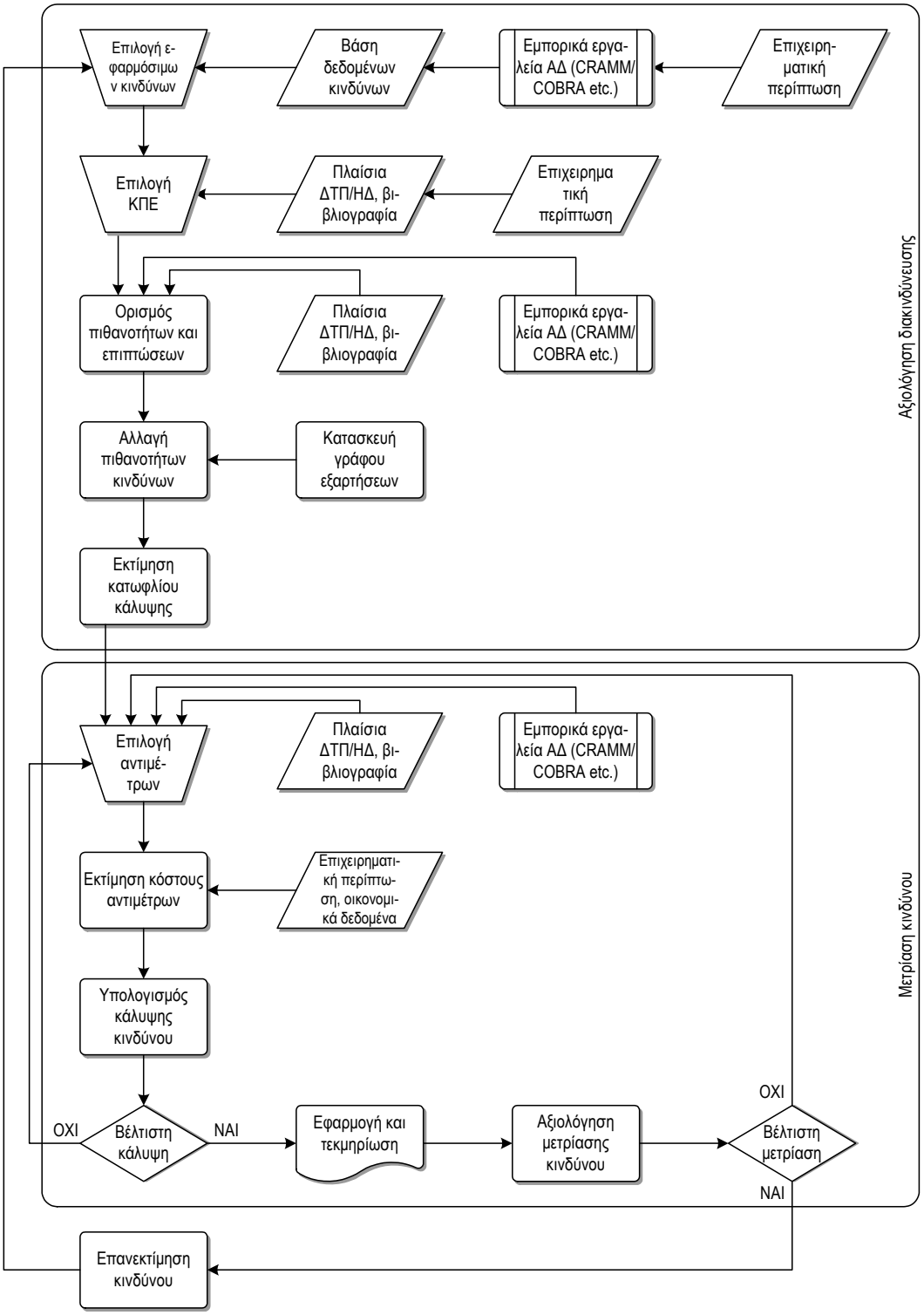
Καθώς, σε αυτό το σημείο ο κίνδυνος και η κάλυψή του είναι ουσιαστικά προβλεπόμενος και εικαζόμενος, σύμφωνα με τις εμπειρίες, τις απόψεις, την κρίση, την κατάρτιση και τις ικανότητες των αξιολογητών, οι *Ri* και *Ci* είναι σαν αποτέλεσμα υποκείμενοι στην άποψή τους. Μαζί με τη μήτρα RIPC^4, αποτελούν ένα εργαλείο εκτίμησης, ειδικευμένο όμως για να καλύψει το χώρο του αποτελεσματικά και με συνέπεια. Οι δείκτες που εισάγει η προτεινόμενη μεθοδολογία έχουν κάποιες ομοιότητες με αυτούς που χρησιμοποιούνται στα CRAMM και COBRA, καθώς και σε μερικές από τις ποιοτικές μεθοδολογίες ΑΔ που παρουσιάστηκαν προηγουμένως, έχει όμως καταβληθεί προσπάθεια να απλοποιηθούν και να προσαρμοστούν στο πεδίο των έργων ΗΔ.

Έχοντας ολοκληρώσει τον υπολογισμό, η ομάδα ΑΔ προχωρά στην τεκμηρίωση και στην υλοποίηση των αντιμέτρων, εντός των κανονικών πλαισίων της διαδικασίας εκτέλεσης του έργου. Ωστόσο, όπως έχει τονιστεί ήδη, η ΑΔ πρέπει να αποτελεί κυκλική επαναληπτική διαδικασία. Ακολουθεί αξιολόγηση της μετρίασης κινδύνου που παρείχε η κάλυψη των αντιμέτρων που επιλέγηκαν, τόσο κατά τη διάρκεια, όσο και μετά την ολοκλήρωση του έργου, η οποία με τη σειρά της ακολουθείται, είτε από επανεπιλογή αντιμέτρων, εφόσον δεν επιτεύχθηκε βέλτιστη μετρίαση, είτε από επαναξιολόγηση των κινδύνων, εφόσον επιτεύχθηκε.

Ο πλήρης αλγόριθμος εφαρμογής της RIPC^4 παρουσιάζεται στο Σχήμα 5, όπου οπτικοποιείται η θέση της μεθοδολογίας εντός της διαδικασίας ΑΔ, τα σημεία διεπαφής και αλληλεπίδρασης με εμπορικά εργαλεία ΑΔ και πλαίσια ΔΤΠ, καθώς και τα δεδομένα που ανταλλάσει με αυτά.

3.2 Αλληλεξάρτηση κινδύνων

Στην παραπάνω μελέτη, έγινε η υπόθεση ότι οι επιμέρους κίνδυνοι είναι ανεξάρτητοι μεταξύ τους, κάτι όμως μάλλον σπάνιο σε πραγματικές συνθήκες. Είναι πολύ συνηθισμένο στα πλαίσια ενός έργου κάποιοι κίνδυνοι να εξαρτώνται από άλλους, δημιουργώντας κάποιας μορφής ιεραρχία, όπου η πραγματοποίηση ενός προκαλεί (συχνά υπό μορφή ντόμινο) την πραγματοποίηση άλλων, ή τουλάχιστον επηρεάζει την πιθανότητά τους να συμβούν. Αντίστροφα, η πιθανότητα ενός κινδύνου επηρεάζεται από τις πιθανότητες άλλων, είτε στην ίδια ομάδα, είτε μεταξύ διαφορετικών ομάδων (Kefallinos et al., 2011).



Σχήμα 5. *Αλγόριθμος εφαρμογής της RIPC*[4]

Προκειμένου να υπολογιστούν οι νέες πιθανότητες, θα χρησιμοποιηθεί ο τύπος του Bayes για την πιθανότητα υπό συνθήκη (conditional probability), όπου η (πρότερη) πιθανότητα ενός γεγονότος τροποποιείται από το ενδεχόμενο μιας υπόθεσης (ή νεότερων δεδομένων) για να παραχθεί μια νέα (μετέπειτα) πιθανότητα του γεγονότος. Εφαρμόζο-

ντας το θεώρημα στην περίπτωσή μας και έχοντας καθορίσει την πρότερη πιθανότητα ενός εξαρτημένου κινδύνου, πρέπει να βρούμε το ενδεχόμενο πραγμάτωσης αυτών από τους οποίους εξαρτάται, παραδεχόμενη την πρότερη πραγματοποίηση του εξαρτημένου, προκειμένου να υπολογίσουμε την μετέπειτα πιθανότητά του.

Ως παράδειγμα, στην περίπτωση δύο κινδύνων *j* και *k* και των πρότερων πιθανοτήτων τους P_{j} και P_{k}, όπου η πραγματοποίηση του *j* επηρεάζεται από τον *k*, έτσι ώστε η πιθανότητα να P_{j} επηρεάζεται από την πιθανότητα P_{k}, πρέπει πρώτα να υπολογίσουμε το ενδεχόμενο $L_{\mathrm{k.j}}$ ότι *ο κίνδυνος k θα λάβει χώρα*, αποδεχόμενοι την υπόθεση ότι *ο κίνδυνος j έχει ήδη λάβει χώρα* (ενδεχόμενο αντίστροφης πραγμάτωσης). Όπως οι αρχικές πιθανότητες, αυτό μπορεί να καθοριστεί με χρήση συστημάτων υποστήριξης αποφάσεων που χρησιμοποιούν AHP ή BBN, με επιπρόσθετη υποστήριξη από ιστορικά δεδομένα και προσωπική εμπειρία πεδίου. Έχοντας καθορίσει το ενδεχόμενο αυτό, η μετέπειτα πιθανότητα $P_{\mathrm{j.k}}$ του κινδύνου *j* δίνεται από την έκφραση:

$$P_{j.k} = \frac{L_{k.j} P_j}{P_k}$$

Στην περίπτωση της εξάρτησης του κινδύνου *j* από δύο άλλους κινδύνους *k* και *m*, με πρότερες πιθανότητες P_{j}, P_{k} και P_{m} αντίστοιχα, έχοντας πρώτα καθορίσει τα (αντίστροφα) ενδεχόμενα $L_{\mathrm{k.j}}$, $L_{\mathrm{m.k}}$ και $L_{\mathrm{m.k.j}}$ της πραγματοποίησης των κινδύνων *k*, *m* και *m* αντίστοιχα, δεδομένου ότι οι κίνδυνοι *j*, *k*, και *k και j* έχουν ήδη λάβει χώρα, η μετέπειτα πιθανότητα $P_{\mathrm{j.k.m}}$ του κινδύνου *j* δίνεται από την έκφραση:

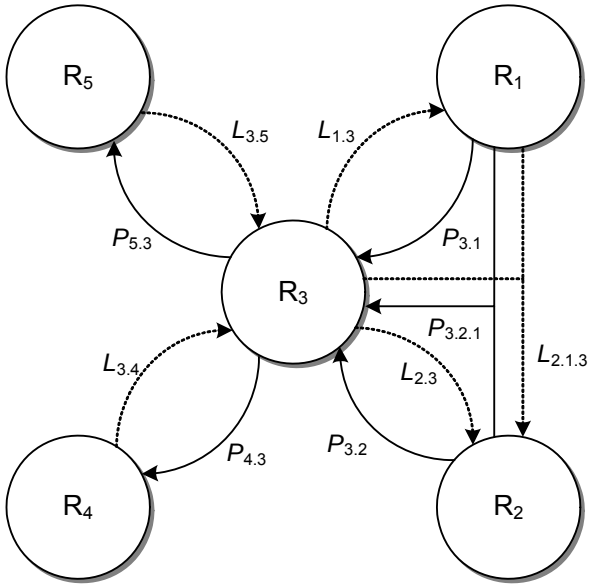
$$P_{j.k.m} = \frac{P_j L_{k.j} L_{m.k.j}}{P_k L_{m.k}}$$

Το παράδειγμα δείχνει ότι πέρα από δύο εξαρτήσεις, ο υπολογισμός γίνεται πολύπλοκος, απαιτώντας ειδικευμένα υπολογιστικά εργαλεία. Συνεπώς, προτείνεται η δημιουργία ενός γράφου αλληλεξάρτησης κινδύνων (risk dependency graph), στον οποίο θα καταβληθεί προσπάθεια να περιοριστεί το μέγιστο μονοπάτι σε 3-4 τμήματα και ο μέγιστος αριθμός κλάδων σε 2-3 εξαρτήσεις, λαμβάνοντας υπόψη μόνο τις πιο σημαντικές. Πρόκειται για ένα αντίστροφο διάγραμμα δέντρου (reverse tree diagram) ή ένα κατευθυντικό ακυκλικό γράφο (directed acyclic graph), όπου τα πιο εξαρτημένα συμβάντα είναι προς τα αριστερά και τα λιγότερο εξαρτημένα είναι προς τα δεξιά, με τη μορφή μονά συνδεδεμένου δικτύου (singly connected network) ή πολυδέντρου (polytree).

Το έργο της κατασκευής του γράφου τοποθετείται αμέσως μετά την επιλογή κινδύνων και τον καθορισμό των αρχικών πιθανοτήτων αυτών, στο δεύτερο βήμα της κατασκευής της μήτρας RIPC[4], του αλγόριθμου εφαρμογής της μεθοδολογίας. Η λογική με την οποία επιλέγονται οι κίνδυνοι που επηρεάζουν έναν τρίτο έχει ως εξής. Επιλέγονται οι κίνδυνοι που:

α) αντίκεινται στους ΚΠΕ ενός κινδύνου και
β) μπορεί να επιδράσουν σε τρωτότητες του συστήματος/έργου που σχετίζονται με ένα κίνδυνο.

Η επιλογή μπορεί να γίνει επίσης με τυπικό εργαλείο ΑΔ, με τη σχετική βιβλιογραφία, με έρευνα στο προσωπικό των φορέων και από εμπειρία πεδίου. Ο γράφος αλληλεξάρτησης κινδύνων μπορεί να θεωρηθεί (και να υπολογιστεί) ως ένα BBN, όπως στο Σχήμα 6, όπου απεικονίζεται ο γράφος αλληλεξάρτησης κινδύνων για πέντε κίνδυνους $R_1 - R_5$, με τις πιθανότητες πραγμάτωσης κάθε κινδύνου $P_{3.1}$, $P_{3.2}$, $P_{5.3}$, $P_{4.3}$, $P_{3.2.1}$, δεδομένης της πραγμάτωσης των κινδύνων που τον επηρεάζουν, καθώς και τα ενδεχόμενα (αντίστροφης) πραγμάτωσης $L_{3.5}$, $L_{3.4}$, $L_{1,3}$, $L_{2.3}$, $L_{2.1.3}$ των κινδύνων, δεδομένης της πραγμάτωσης των εξαρτημένων.



Σχήμα 6. *BBN για πέντε αλληλεξαρτώμενους κινδύνους*

Παρουσιάζοντας τις εξαρτήσεις μεταξύ όλων των κινδύνων, ο γράφος εξάρτησης κάνει δυνατή την εκτίμηση των μονοπατιών κινδύνου ή επίθεσης προς ένα ερ-

γο/σύστημα και μπορεί έτσι να χρησιμοποιηθεί και στα πλαίσια μιας διαδικασίας εκτίμησης τρωτοτήτων.

Ένα πρόβλημα στην κατασκευή του γράφου εξάρτησης και τον υπολογισμό των μετέπειτα πιθανοτήτων των κινδύνων, είναι η εκτίμηση των ενδεχομένων L ότι κίνδυνοι από τους οποίους υπάρχει εξάρτηση θα λάβουν χώρα, δεδομένου ότι οι κίνδυνοι που εξαρτώνται έχουν ήδη λάβει χώρα ($L_{\mathrm{k.j}}$, $L_{\mathrm{m.k}}$ και $L_{\mathrm{m.k.j}}$ στους προηγούμενους τύπους). Στο παράδειγμα του Σχήματος 3, αν δεχτούμε ότι ο κίνδυνος R_{i} έχει πραγματωθεί, μπορούμε να υπολογίσουμε τις πιθανότητες να ισχύουν οι παράγοντες F_{i1} και F_{i2} ως εξής:

$$
\begin{aligned}
L_{F_{i2}.R_i} &= P(F_{i2} \mid R_i) = \frac{(P(R_i \mid F_{i2}) \cdot P(F_{i2}))}{P(R_i)} \\
&= \frac{((P(R_i \mid F_{i1}, F_{i2}) \cdot P(F_{i1}) + P(R_i) \mid F'_{i1}, F_{i2}) \cdot P(F'_{i1})) \cdot P(F_{i2})}{P(R_i)} \\
&= \frac{(0{,}8 \cdot 0{,}1 + 0{,}5 \cdot 0{,}9) \cdot 0{,}4}{0{,}518} \\
&= 0{,}409
\end{aligned}
$$

$$
\begin{aligned}
L_{F_{i1}.R_i} &= P(F_{i1} \mid R_i) = \frac{(P(R_i \mid F_{i1}) \cdot P(F_{i1}))}{P(R_i)} \\
&= \frac{(P(R_i \mid F_{i1}, F_{i2}) \cdot P(F_{i2}) + P(R_i \mid F_{i1}, F'_{i2}) \cdot P(F'_{i2})) \cdot P(F_{i1})}{P(R_i)} \\
&= \frac{(0{,}8 \cdot 0{,}4 + 0{,}6 \cdot 0{,}6) \cdot 0{,}1}{0{,}518} \\
&= 0{,}131
\end{aligned}
$$

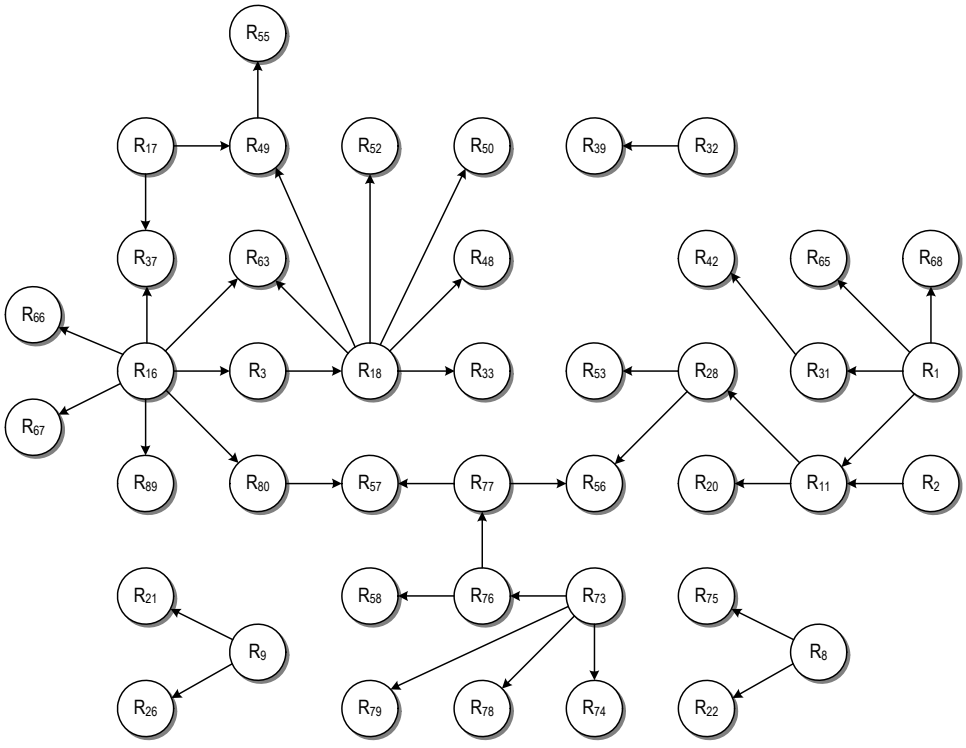
Έχοντας υπολογίσει τις μετέπειτα πιθανότητες των εξαρτημένων κινδύνων, η ομάδα αξιολόγησης θα προχωρήσει στο τρίτο βήμα του αλγόριθμου εφαρμογής της RIPC[4], την επιλογή αντιμέτρων.

Για τη διευκόλυνση των αξιολογητών και σαν μέρος του εργαλείου εφαρμογής ΑΔ που συνοδεύει την προτεινόμενη μεθοδολογία, στο Σχήμα 7 προτείνονται αλληλεξαρτήσεις και μονοπάτια κινδύνου, χωρίς όμως να περιορίζονται οι αξιολογητές στο να ορίσουν δικές τους εξαρτήσεις και μονοπάτια, κατά βούληση. Επιπλέον, στον Πίνακα 3 του Παραρτήματος Α προτείνονται και ενδεχόμενα μονής εξάρτησης (στο οριζόντιο είναι ο επηρεαζόμενος κίνδυνος και στο κάθετο αυτός που τον επηρεάζει), σύμφωνα με την κρίση του συγγραφέα για το ποιά είναι τα πιο σημαντικά, τις οποίες μπορούν επίσης να προσαρμόσουν και να χρησιμοποιήσουν οι αξιολογητές.

3.3 Προέκταση στην 3η διάσταση: σύνδεση με άλλα έργα

Στην αρχική μορφή της μεθοδολογίας, έγινε η υπόθεση ότι το εξεταζόμενο έργο ΗΔ εκτελείται μοναδιαία και αποτιμάται αυτόνομα. Ως αποτέλεσμα οι πιθανότητες των κινδύνων βάσει των οποίων υπολογίζεται ο δείκτης διακινδύνευσης *Ri* είναι ανεξάρτητες μεταβλητές, μεταξύ τους και από άλλους κίνδυνους, ίδιους ή άλλους του ιδίου ή άλλου έργου. Ωστόσο, όπως έχει ήδη αναφερθεί, σπάνια συμβαίνει αυτό· τις περισσότερες φορές πολλαπλά έργα εκτελούνται παράλληλα, αλληλεπικαλυπτόμενα, ή σε ακολουθία, αλλά όπως και να έχει με τρόπο που επηρεάζουν το ένα το άλλο. Ο επηρεασμός μεταξύ έργων οφείλεται τυπικά στη χρήση κοινών υλικών, διαδικασιών ή ατόμων σε ένα ή περισσότερα από τα παρακάτω επίπεδα:

α) του φορέα υλοποίησης,
β) του ανάδοχου/εργολάβου,
γ) υλικών/υπηρεσιών,
δ) διοίκησης/ηγεσίας και
ε) οικονομικών/χρηματοδότησης.

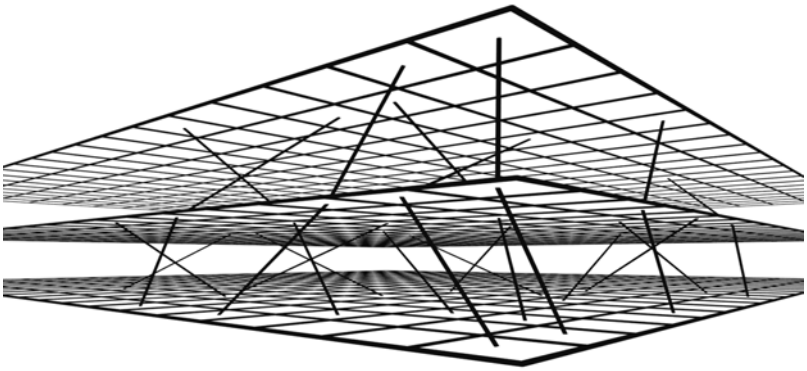


Σχήμα 7. *Προτεινόμενες αλληλεξαρτήσεις και μονοπάτια κινδύνου*

Στην προηγούμενη ενότητα δείξαμε πως οι αλληλεξαρτήσεις των κινδύνων μπορούν να συμπεριληφθούν στους υπολογισμούς διατίμησης του συνολικού κινδύνου για ένα

έργου. Σε αυτό το σημείο θα επεκτείνουμε τη μεθοδολογία μας σε περισσότερα του ενός έργα.

Η ανάλυση πολλαπλών έργων μπορεί να αντιμετωπιστεί ως πολλαπλές μήτρες RIPC^4 σε ένα χώρο τριών διαστάσεων (ή μια μήτρα τριών διαστάσεων), όπου κάθε επίπεδο αναπαριστά ένα έργο και όπου οι πιθανότητες των κινδύνων σε ένα έργο-επίπεδο, επηρεάζουν τις πιθανότητες των κινδύνων σε ένα ή περισσότερα επίπεδα. Το Σχήμα 8 οπτικοποιείται η αλληλεξάρτηση των κινδύνων μεταξύ έργων, σαν σχέσεις μεταξύ δισδιάστατων επιπέδων στον τρισδιάστατο χώρο. Η μήτρα RIPC^4 ενός έργου αποτελεί ένα επίπεδο.



Σχήμα 8. *Οπτικοποίηση τρισδιάστατης μήτρας κινδύνων-εξαρτήσεων*

Αυτό μπορεί να δημιουργήσει ένα πολύπλοκο σχήμα αίτιου-αιτιατού, καθιστώντας τον υπολογισμό των μετέπειτα πιθανοτήτων των κινδύνων δύσκολο. Και ενώ είναι δυνατό, με ειδικευμένο εργαλείο να υπολογιστούν οι μετέπειτα πιθανότητες λαμβάνοντας υπόψη εξαρτήσεις ανάμεσα σε έργα (περιλαμβάνοντας απλώς κινδύνους και από άλλα έργα στον γράφο αλληλεξάρτησης κινδύνων), σε αυτό το σημείο θα εισάγουμε μια απλοποίηση: θα υποθέσουμε ότι ένας κίνδυνος ενός έργου μπορεί να επηρεάσει μόνο τον αντίστοιχο κίνδυνο σε ένα άλλο έργο. Αυτό βασίζεται στην παρατήρηση ότι στην πράξη, όταν τρέχουν πολλά παράλληλα έργα μέσα στον ίδιο οργανισμό ή με τους ίδιους αποδέκτες/χρήστες, συγκεκριμένα είδη ενεργειών ή υπηρεσιών ανατίθενται, ή αφορούν, ή χρησιμοποιούνται από τις ίδιες ομάδες ανθρώπων, συνήθως με βάση την ειδίκευση, τη θέση, την υπευθυνότητα ή το ενδιαφέρον. Για παράδειγμα, η συγγραφή της αρχιτεκτονικής δικτύου και των χαρακτηριστικών υλικού ανατίθενται σε μηχανικούς hardware, ενώ η οργάνωση και η δομή μιας υπηρεσίας υποστήριξης (help desk) στο προσω-

πικό ανθρωπίνων πόρων (human resources). Οπωσδήποτε, αυτή η απλοποίηση μπορεί να μειώνει τον αριθμό των εξαρτήσεων και γι' αυτό είναι προαιρετική· η ομάδα ΑΔ μπορεί να επιλέξει να αντιμετωπίσει τη δυσκολία του να λάβει υπόψη όλες τις πιθανές εξαρτήσεις κινδύνων, επεκτείνοντας τον γράφο αλληλεξάρτησης ανάμεσα στα επίπεδα, διασυνδέοντας κινδύνους από πολλαπλά έργα.

Στην προηγούμενη ενότητα, για την αναπαράσταση των εξαρτήσεων εντός ενός έργου, προτάθηκε η χρήση γράφου αλληλεξάρτησης κινδύνων σε μορφή αντίστροφου διαγράμματος δέντρου, με τους πιο εξαρτημένους κίνδυνους στα αριστερά και τους λιγότερο στα δεξιά, με προσπάθεια να περιοριστεί το μέγιστο μονοπάτι σε δύο ή τρία τμήματα και ο μέγιστος αριθμός κλάδων σε δύο ή τρεις εξαρτήσεις. Στην περίπτωση πολλαπλών έργων, οι εξαρτήσεις του γράφου θα πρέπει να αναπαριστούν τις εξαρτήσεις κινδύνων μεταξύ έργων. Επειδή όμως μπορεί να μην ισχύουν για όλους τους κινδύνους ενός έργου, γιατί μπορεί να μην έχουν εξαρτήσεις εκτός έργου, τα απλά αριθμητικά ενδεχόμενα του Σχήματος 8 θα αντικατασταθούν από διανύσματα ενδεχομένων, μία τιμή για κάθε ζεύγος κινδύνων που «συμμετέχουν» στην εξάρτηση.

Η ομάδα εμπειρογνωμόνων ακολουθεί τα ίδια βήματα της RIPC[4], καθορίζοντας τους κινδύνους, τις πιθανότητές τους, τις επιπτώσεις, τους ΚΠΕ, τα αντίμετρα και τα κόστη τους, τα κατώφλια κάλυψης και τις καλύψεις, όπως και τους δείκτες *Ri*, *Ci*, *Mi* και *Co*. Σε ένα επιπλέον βήμα, αμέσως μετά το δεύτερο, γίνεται η κατασκευή του γράφου αλληλεξάρτησης και η μεταβολή των πιθανοτήτων των κινδύνων ενός έργου, λαμβάνοντας υπόψη τις πιθανότητες των κινδύνων του έργου από το οποίο εξαρτάται. Όπως και στην προηγούμενη ενότητα, αυτό γίνεται με τον τύπου του Bayes της υπό συνθήκη πιθανότητας. Στην περίπτωση των αλληλεξάρτησης μεταξύ δύο έργων 1 και 2:

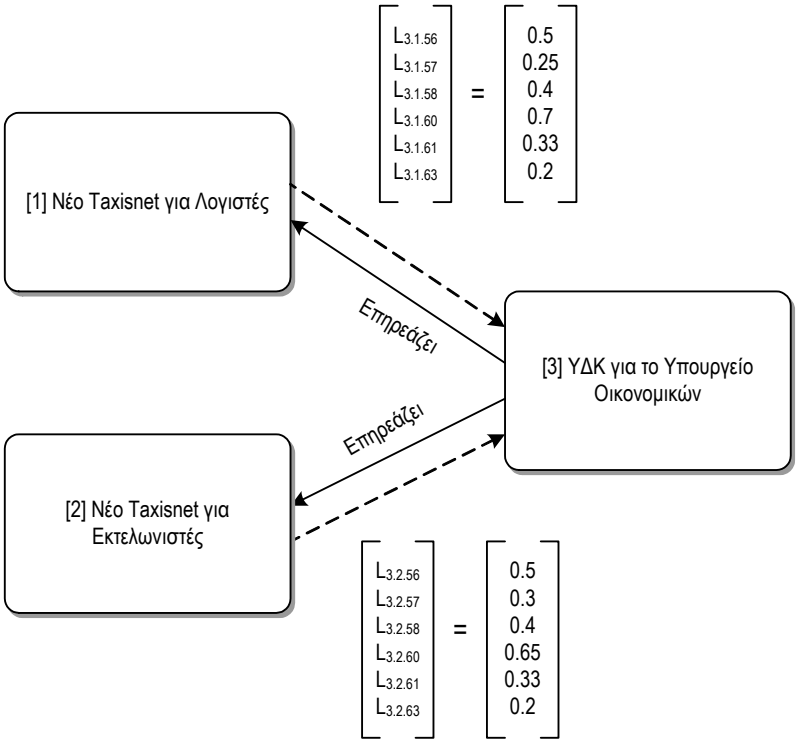
$$P_{1.2.j} = \frac{L_{2.1.j} P_{1.j}}{P_{2.j}}$$

όπου $P_{1.2.\mathrm{j}}$ είναι η μετέπειτα πιθανότητα του κίνδυνου *j* στο έργο 1, δεδομένου ότι εξαρτάται από τον ίδιο κίνδυνο στο έργο 2, $P_{1.\mathrm{j}}$ η πρότερη πιθανότητα του κίνδυνου *j* στο έργο 1, $P_{2.\mathrm{j}}$ η πρότερη πιθανότητα του κίνδυνου *j* στο έργο 2 και $L_{2.1.\mathrm{j}}$ το ενδεχόμενο ότι ο κίνδυνος *j* θα πραγματωθεί στο έργο 2, με την παραδοχή ότι ο ίδιος κίνδυνος *j έχει ήδη* πραγματωθεί στο έργο 1. Για τρία έργα που σχετίζονται, όπου το πρώτο έχει εξάρτηση από τα δύο άλλα, η έκφραση γίνεται:

$$P_{1.2.3.j} = \frac{P_{1.j} L_{2.1.j} L_{3.1.2.j}}{P_{2.j} L_{3.2.j}}$$

όπου $P_{1.2.3.j}$ είναι η μετέπειτα πιθανότητα του κίνδυνου *j* στο έργο 1, δεδομένου ότι εξαρτάται από τον ίδιο κίνδυνο στα έργα 2 και 3, $P_{1.j}$ η πρότερη πιθανότητα του κίνδυνου *j* στο έργο 1, $P_{2.j}$ η πρότερη πιθανότητα του κίνδυνου *j* στο έργο 2, $L_{2.1.j}$ το ενδεχόμενο ότι ο κίνδυνος *j* θα λάβει χώρα στο έργο 2, δεδομένου ότι έχει ήδη λάβει χώρα στο έργο 1, $L_{3.1.2.j}$ το ενδεχόμενο ότι ο κίνδυνος *j* θα λάβει χώρα στο έργο 3, με την παραδοχή ότι *έχει ήδη* λάβει χώρα στα έργα 1 και 2 και $L_{3.2.j}$ το ενδεχόμενο ότι ο κίνδυνος *j* θα λάβει χώρα στο έργο 3, με την παραδοχή ότι *έχει ήδη* λάβει χώρα στο έργο 2.

Ως παράδειγμα της αλληλεξάρτησης (κινδύνων) έργων, παρουσιάζουμε τη σχέση μεταξύ ενός έργου Υποδομής Δημοσίου Κλειδιού για το Υπουργείο Οικονομικών και δύο έργα για ολοκληρωμένες εφαρμογές βασισμένες στον Ιστοχώρο, για ιδιωτικά λογιστικά γραφεία (TaxisNet για Λογιστές) και ιδιωτικά γραφεία εκτελωνισμού (TaxisNet για Εκτελωνιστές). Λόγω της φύσης του, αλλά και της λειτουργικής εξάρτησης (έκδοση, χρήση και διαχείριση ψηφιακών πιστοποιητικών χρηστών) οι κίνδυνοι του έργου της ΥΔΚ επηρεάζουν παρόμοιους κινδύνους των άλλων έργων, ιδιαίτερα στις περιοχές της εμπιστοσύνης των χρηστών και των κινήτρων χρήσης (της υποδομής). Στο Σχήμα 9 παρουσιάζεται απόσπασμα του γράφου εξάρτησης μεταξύ τριών έργων, εστιάζοντας στο επίπεδο τελικού χρήστη της μήτρας RIPC[4], με τα διανύσματα ενδεχομένων και συμμετοχής στην εξάρτηση. Σε αυτή την εικόνα, ακολουθούμε τη σημειογραφία που περιγράφεται προηγουμένως, όπου το έργο 3 είναι το έργο ΥΔΚ, το έργο 1 είναι το TaxisNet για λογιστές και το έργο 2 είναι το TaxisNet για Εκτελωνιστές. Τα δύο διανύσματα ενδεχομένων αντιπροσωπεύουν και τους κινδύνους που συμμετέχουν στη σχέση εξάρτησης των έργων και τις τιμές των (αντίστροφων) πιθανοτήτων.



Σχήμα 9. *Παράδειγμα γράφου αλληλεξάρτησης έργων*

Η σελίδα αυτή είναι σκόπιμα λευκή

ΚΕΦΑΛΑΙΟ 4

Περιπτώσεις εφαρμογής: ΥΔΚ-ΣΥΖΕΥΞΙΣ και Πρωτότυπη ΥΔΚ

Η σελίδα αυτή είναι σκόπιμα λευκή

Σε αυτό το κεφάλαιο της διατριβής, παρουσιάζονται δύο περιπτώσεις εφαρμογής της προτεινόμενης μεθοδολογίας ΑΔ, μία στην ΥΔΚ-ΣΥΖΕΥΞΙΣ (Kefallinos et al., 2006) και μία σε πρότυπη ΥΔΚ που προστατεύει τα προσωπικά δεδομένα και διασφαλίζει την ελευθερία βούλησης των ατόμων (Kefallinos & Sykas, 2012). Για να τοποθετηθούν στο περιβάλλον τους, πρώτα παρουσιάζονται εν συντομία οι δύο ΥΔΚ και μετά γίνονται οι εφαρμογές. Στο πρώτο τμήμα του κεφαλαίου παρουσιάζεται το έργο ΣΥΖΕΥΞΙΣ, στην πρώτη και στην δεύτερη υλοποίησή του και αναλύεται η ΥΔΚ που αποτέλεσε το υποέργο 9 του ΣΥΖΕΥΞΙΣ-1. Στη συνέχεια, εφαρμόζεται η προτεινόμενη μεθοδολογία ΑΔ στο τμήμα του έργου που αφορά τους κινδύνους επιπέδου τελικού χρήστη. Στο δεύτερο τμήμα του κεφαλαίου, παρουσιάζεται η πρότυπη ΥΔΚ και μετά εφαρμόζεται η μεθοδολογία στο τμήμα του έργου που αφορά τους κινδύνους επίπεδου πολιτικής ηγεσίας. Τέλος εξάγονται συμπεράσματα από την εφαρμογή της προτεινόμενης μεθοδολογίας και στις δύο περιπτώσεις εφαρμογής.

4.1 ΥΔΚ-ΣΥΖΕΥΞΙΣ

4.1.1 Γενική περιγραφή ΣΥΖΕΥΞΙΣ και ΥΔΚ-ΣΥΖΕΥΞΙΣ

Το έργο ΣΥΖΕΥΞΙΣ είναι ένα έργο υποδομής επικοινωνιών και πληροφοριακών συστημάτων μεγάλης κλίμακας για την Ελληνική Δημόσια Διοίκηση (ΕΔΔ), που καλύπτει ολόκληρη την Ελληνική επικράτεια. Στην πιλοτική του φάση (2001-2005) κάλυπτε 35 κτήρια σε 10 πόλεις, στη φάση ΣΥΖΕΥΞΙΣ-1 (2006-2011) 4.485 κτήρια σε 6 νησίδες σε όλες σχεδόν τις πόλεις της Ελλάδος και στην υπό υλοποίηση φάση ΣΥΖΕΥΞΙΣ-2 (2012-2016) σχεδόν 33.000 κτήρια σε 9 νησίδες (συν μία ασύρματη) σε όλες τις πόλεις της Ελλάδος. Υπολογίζεται ότι κάθε χρόνο που θα λειτουργεί, το ΣΥΖΕΥΞΙΣ-2 θα εξοικονομεί 155 εκ. €, με όφελος πάνω από 50% στις τηλεπικοινωνίες. Αυτό το φιλόδοξο έργο εξυπηρετεί όλους τους τομείς της ΕΔΔ, μεταξύ των οποίων το Υπουργείο Εσωτερικών (κεντρικά, γενικές γραμματείες, περιφέρειες, δήμοι και ΚΕΠ), το Υπουργείο Οικονομικών (κεντρικές υπηρεσίες, ΔΟΥ, τελωνεία), το Υπουργείο Άμυνας και το Υπουργείο Υγείας.

Ο κύριος στόχος του ΣΥΖΕΥΞΙΣ είναι η βελτίωση της υποδομής και των λειτουργιών της ΕΔΔ, με αναβάθμιση των τηλεπικοινωνιακών υπηρεσιών, παροχή σύγχρονης τεχνολογίας της πληροφορίας και ασφάλειας και μείωση του κόστους μέσα από οικονομία κλίμακας. Αποτελεί στο σύνολό του, μια από τις κύριες ωθήσεις για τη διαμόρ-

φωση των κατάλληλων υποδομών και υπηρεσιών, προς την ανάπτυξη της ΗΔ στην Ελλάδα.

Το ΣΥΖΕΥΞΙΣ-1 χωρίζεται σε εννέα μικρότερα υποέργα, από τα οποία τα επτά αφορούν την οργάνωση και την κατασκευή του δικτύου τηλεπικοινωνιών, ένα αφορά την εκπαίδευση των χρηστών και το ένατο την υπηρεσία ΥΔΚ. Το ΣΥΖΕΥΞΙΣ-2 επικεντρώνεται στην αναβάθμιση και τη βελτίωση της τηλεπικοινωνιακής υποδομής του ΣΥΖΕΥΞΙΣ-1, εστιάζοντας στην υπηρεσία δικτυακής πρόσβασης (διανομή και κορμός) και στην υπηρεσία τηλεφωνίας (παροχή κεντρικής information management service – IMS). Κάθε κτήριο ταξινομείται με βάση δύο χαρακτηριστικά του, την ταχύτητα πρόσβασης στο δίκτυο και το προφίλ τηλεφωνίας. Επιπλέον, παρέχονται: δυνατότητα μικρότερης ταχύτητας πρόσβασης για το 5% των μικρών φορέων για ένα έτος, υποχρέωση παροχής αυξημένης ζητούμενης ταχύτητας πρόσβασης στα σημεία που είναι εφικτή η χρήση υποδομών metro area network (MAN) και επικαιροποίηση της ζήτησης (εύρος και είδος) κατά τη μελέτη εφαρμογής. Στα 3689 κτήρια (68 πόλεις) πανελλαδικά που υπάρχει πρόσβαση MAN, παροχή κυρίως 100 Mbps, αλλά και 1 Gbps.

Οι υπηρεσίες πρόσβασης χωρίζονται στις ακόλουθες κατηγορίες:

α) *Ασύμμετρη:* Ταχύτητα 24/1 Mbps (download/upload). Τεχνολογία ADSL. Προϋπολογισμός 20.519 φορείς.

β) *Μικρή:* Ταχύτητα 10/10 Mbps συμμετρική. Τεχνολογίες Metro Ethernet, VDSL, EFM, radio access, ADSL backup. Προϋπολογισμός 8.181 φορείς.

γ) *Μεσαία:* Ταχύτητα 100/100 Mbps συμμετρική. Τεχνολογίες Metro Ethernet διπλής σύνδεσης (dual-homed), μονής πρόσβασης (single-access). Προϋπολογισμός 331 φορείς, 3.674 φορείς με πρόσβαση MAN.

δ) *Μεγάλη:* Ταχύτητα 1/1 Gbps συμμετρική. Τεχνολογίες Metro Ethernet διπλής σύνδεσης, διπλής πρόσβασης (dual-access). Προϋπολογισμός 100 φορείς, 15 φορείς με πρόσβαση MAN.

Σύνολο προϋπολογιζόμενων φορέων: 32.820.

Στο αντικείμενο του ΣΥΖΕΥΞΙΣ-2 περιλαμβάνεται η δημιουργία δύο κεντρικών κόμβων (SIX-1 και SIX-2) για τη διασύνδεση υποδομών και υπηρεσιών του ΣΥΖΕΥΞΙΣ-2, η 15ετής μίσθωση ινών (σκοτεινή ίνα) για τη σύνδεση των κόμβων μεταξύ τους και με το GRIX, δύο συνδέσεις προς το Διαδίκτυο (Internet feed) των 5 Gbps ανά κόμβο για 3 έτη, καθώς και υπηρεσίες λειτουργίας και υποστήριξης της συνολικής υποδομής για 3 έτη. Οι δύο κεντρικοί κόμβοι θα βρίσκονται σε διαφορετικά data centers, θα είναι ταυτόχρονα ενεργοί (active-active) και ισοδύναμοι (δηλαδή θα μπορεί ο καθένας

να αναλάβει το σύνολο του φορτίου του δικτύου) και θα διαθέτουν διπλές οπτικές συνδέσεις μεταξύ τους των 40 GE με ξεχωριστές οδεύσεις. Οι κεντρικοί κόμβοι θα περιλαμβάνουν: α) δύο δρομολογητές κορμού κλάσης terabit με διεπαφές 4x40 GE (διασύνδεση), 25x 10GE (σύνδεση μέχρι 25 νησίδων) και 8x GE (σύνδεση με GRIX, sTESTA, ΔΙΑΣ), β) δύο κεντρικούς μεταγωγείς και γ) την υποδομή ολοκλήρωσης υπηρεσιών πολυμέσων (IMS). Για το SIX-1 έχει προβλεφθεί μίσθωση χώρου σε collocation data center (μαζί με τις κεντρικές υποδομές του ΣΥΖΕΥΞΙΣ-2), ενώ το SIX-2 θα φιλοξενηθεί σε data center του δημοσίου (σε απόσταση τουλάχιστον 10 χλμ).

Για την υπηρεσία της τηλεφωνίας, θα παρέχεται ο κεντρικός εξοπλισμός και υποδομή (IMS, SIP, T.38, H.323), φορητότητα αριθμών, μία τηλεφωνική γραμμή και συσκευή ανά κτήριο για κλήσεις προς το helpdesk, χρήση υφιστάμενου τηλεφωνικού εξοπλισμού και επιπρόσθετου από το υποέργο 11, διεπαφή με το IMS του SIX και πακέτο χρήσης τηλεφωνίας ανά νησίδα. Όσον αφορά το τελευταίο, εντός του προϋπολογισμού του έργου είναι η επικοινωνία εντός ΣΥΖΕΥΞΙΣ (onnet), προς κινητά υποέργου ασύρματης νησίδας, εκτός ΣΥΖΕΥΞΙΣ-2 εντός Ελλάδος αστικοί και υπεραστικοί προορισμοί και εκτός ΣΥΖΕΥΞΙΣ-2 πακέτο για κινητές, διεθνείς και ολιγοψήφιες κλήσεις. Κάθε τρίμηνο θα γίνεται επαναδιαπραγμάτευση των πακέτων. Θα συνεχίσουν να παρέχονται υπηρεσίες τηλεσυνδιάσκεψης, τηλεσυνεργασίας και καταλόγου.

Όσον αφορά τη διασύνδεση της υπηρεσίας διανομής (νησίδα) με την κεντρική υποδομή, καθορίζονται υποδομή IP/MPLS, πολλαπλά VPN δεδομένων, VPN υπηρεσιών και προτεραιοτήτων (QoS – CoS), υποδομή διασύνδεσης των PoP των MAN με τα PoP διανομής και δύο κυκλώματα (ένα προς κάθε κόμβο SIX) τουλάχιστον 10 Gbps. Η εσωτερική αρχιτεκτονική της νησίδας γίνεται μέσω του ιδιόκτητου δικτύου του αναδόχου και χρήση των υποδομών της πρόσκλησης ’98. Πάνω στις νησίδες συνδέονται οι φορείς του δημοσίου, τουλάχιστον ένας ανά νησίδα, με δυνατότητα καθορισμού διακριτικής πρόσβασης, εντός και εκτός της νησίδας.

Όσον αφορά το υποέργο της ασύρματης πρόσβασης, έχει προϋπολογισθεί η παροχή σύνδεσης ADSL σε 400 υφιστάμενα δημόσια hotspots για 3 χρόνια, ενώ δεν βρίσκονται εντός του έργου η παροχή υπηρεσίας εγκατάστασης μόνιμων δικτυακών υποδομών διασύνδεσης μεταξύ κτηρίων με τεχνολογία wifi/wimax, η παροχή υπηρεσίας ασύρματης δικτυακής κάλυψης χώρου εκδηλώσεων με wifi hotspot και η παροχή υπηρεσιών δημοσίων hotspots σε νέα σημεία.

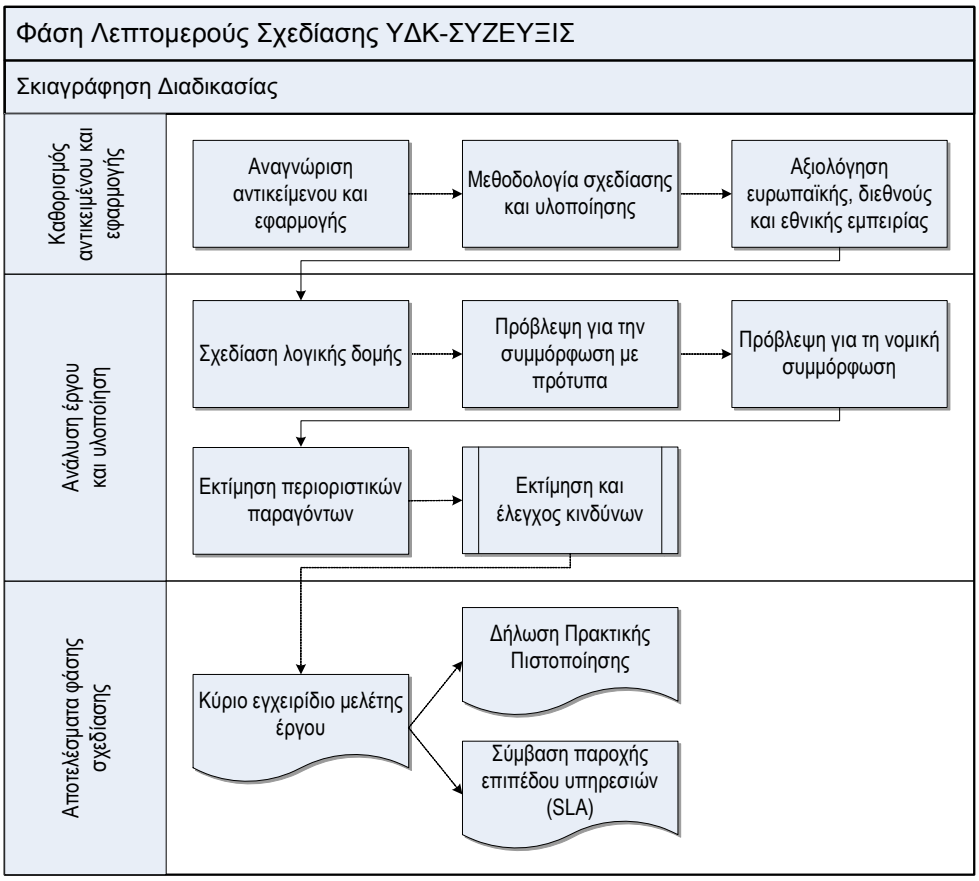
Συνολικά τα τρέχοντα ετήσια λειτουργικά τηλεπικοινωνιακά κόστη της ΕΔΔ (φωνή και δεδομένα) κυμαίνονται μεταξύ 250 και 300 εκ € και το ΣΥΖΕΥΞΙΣ-2 θα παρέχει σημαντικά αναβαθμισμένες υπηρεσίες με ετήσιο κόστος 150 εκ. €.

Ειδικότερα για την υπηρεσία ΥΔΚ του υποέργου 9 του ΣΥΖΕΥΞΙΣ-1 (Kefallinos et al., 2006), η ΕΔΔ επέλεξε να μην υλοποιήσει αυτή την υπηρεσία με ίδιους πόρους, αλλά να την αναθέσει (outsource) σε ιδιωτικό οργανισμό-πάροχο, όπως κάνουν και πολλές άλλες χώρες ανά τον κόσμο. Η ιδιωτική εταιρία ανέλαβε την υποχρέωση να παρέχει την υποδομή, την τεχνική υλοποίηση και την υποστήριξη των Αρχών Πιστοποίησης (ΑΠ) και Αρχών Εγγραφής (ΑΕ) που εκδίδουν τα πιστοποιητικά για τους τομείς της ΕΔΔ και των χρηστών. Την υπηρεσία διαχειρίζεται και λειτουργεί το προσωπικό συγκεκριμένης δημόσιας υπηρεσίας (Αρχή Πιστοποίηση Ελληνικού Δημοσίου – ΑΠΕΔ) που ορίστηκε και εκπαιδεύτηκε από τον πάροχο για λειτουργίες ΑΠ. Η χρήση των πιστοποιητικών υποστηρίζεται από έξυπνες κάρτες (smartcards) και αντίστοιχους αναγνώστες, μοιράστηκαν στους χρήστες.

Εντός του ΣΥΖΕΥΞΙΣ, η ΑΠ είναι η έμπιστη αρχή που διασφαλίζει τους ανωτέρω στόχους και παρέχει το ασφαλές και έμπιστο περιβάλλον, το οποίο απαιτείται για την πραγμάτωση του πλαισίου ΗΔ. Οι κρυπτογραφικές υπηρεσίες που παρέχει (ασύμμετρη κρυπτογράφηση, κατάτμηση και ηλεκτρονικές υπογραφές), εγγυώνται την τήρηση των ανωτέρω αρχών σε πλειάδα ηλεκτρονικών εφαρμογών, όπως ασφαλή ή/και πιστοποιημένη ανταλλαγή πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου, ανταλλαγή εγγράφων, πρόσβαση σε ιστοχώρους της ΕΔΔ και υπηρεσιών της από πολίτες, καθώς και ασφαλή επικοινωνία και συναλλαγές μεταξύ διαφορετικών φορέων της ΕΔΔ και μεταξύ της ΕΔΔ και τρίτων (εταιρίες, ιδιώτες κτλ).

Η μεθοδολογική προσέγγιση για την ανάπτυξη της υπηρεσίας ΥΔΚ-ΣΥΖΕΥΞΙΣ περιλαμβάνει επτά φάσεις, οι οποίες λαμβάνουν χώρα σε όλα τα κύρια επίπεδα των οργανισμών που την αφορούν (Σχήμα 10). Η προσέγγιση αυτή είναι συνεπής με τα διεθνή πρότυπα, διασφαλίζει ότι η υπηρεσία ΥΔΚ ταιριάζει με την οργανωτική και λειτουργική δομή των δημοσίων υπηρεσιών και μεγιστοποιεί (σχεδιαστικά) την πιθανότητα για την αποδοχή και την υιοθέτησή της. Από τις αναφερόμενες φάσεις, αυτή της λεπτομερούς σχεδίασης είναι η πιο σημαντική. Το διάγραμμα ροής της παρουσιάζεται στο Σχήμα 11 και αναλύεται περαιτέρω σε αυτή και στην επόμενη ενότητα.

Σχήμα 10. *Σκιαγράφηση της μεθοδολογίας ανάπτυξης του έργου ΥΔΚ-ΣΥΖΕΥΞΙΣ.*



Σχήμα 11. *Διάγραμμα ροής της φάσης λεπτομερούς σχεδίασης της ΥΔΚ-ΣΥΖΕΥΞΙΣ.*

Κατά την φάση σχεδιασμού της ΥΔΚ-ΣΥΖΕΥΞΙΣ, έγινε επισκόπηση της εφαρμογής και της εμπειρίας σε ΥΔΚ αρκετών χωρών, όπως και διεθνών και εθνικών οργανισμών. Η επιδίωξη ήταν να εξαχθούν χρήσιμα συμπεράσματα για τους στόχους σχεδία-

σης και τα προβλήματα που μπορεί να προκύψουν κατά την υλοποίηση και την αποδοχή της δομής και των πρακτικών μιας ΥΔΚ σε μεγάλο όγκο οργανισμών και ατόμων. Ειδικότερα, εξετάστηκαν οι εθνικές πρωτοβουλίες, απαιτήσεις και υλοποιήσεις των ΥΔΚ του Βελγίου (.beID, 2001), Καναδά (GoC, 2001), Φινλανδίας (FINEID, 2000) και Ολλανδίας (PKIoverheid, 2002). Επίσης εξετάστηκαν η ΥΔΚ του προγράμματος IDA(BC) της ΕΕ [IDA(BC) PKI, 1999] και από τις Ελληνικές προσπάθειες, το σύστημα Ερμής των Ελληνικών Χρηματιστηρίων, το μητρώο EDIRA του Εμπορικού Επιμελητηρίου Αθηνών και η ΥΔΚ που ανέπτυξε το Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών για το Υπουργείο Παιδείας.

Οι κύριες παρατηρήσεις που εξήχθησαν από τα παραπάνω και θεωρήθηκαν χρήσιμα σημεία εστίασης για το έργο της ΥΔΚ-ΣΥΖΕΥΞΙΣ είναι οι ακόλουθες:

α) Οι περισσότερες από τις ευρωπαϊκές και δυτικές χώρες έχουν υιοθετήσει ή κινούνται προς ένα ασφαλές μοντέλο ΗΔ βασισμένο σε ΥΔΚ, τόσο για ιδιώτες όσο και για πολίτες.

β) Η εισαγωγή και χρήση υπηρεσιών πιστοποίησης και ηλεκτρονικών υπογραφών σε ευρεία κλίμακα ξεκίνησε από το δημόσιο τομέα.

γ) Οι τεχνολογικές δυνατότητες που παρέχονται από υπηρεσίες ΥΔΚ έχει ωθήσει τη δημόσια διοίκηση να επανεξετάσει και επαναπροσδιορίσει τις σχέσεις κράτους, εταιριών και πολιτών, φέρνοντας στο προσκήνιο την ΗΔ.

δ) Η κύρια έμφαση στην εφαρμογή υπηρεσιών ΥΔΚ έχει δοθεί στην ασφάλεια συναλλαγών.

ε) Η υλοποίηση μονολιθικού και καθολικού μοντέλου εμπιστοσύνης έχει αποδειχθεί υπερ-φιλόδοξος στόχος, λόγω του υψηλού κόστους των υπηρεσιών ΥΔΚ.

στ) Σε πολλές περιπτώσεις δεν έγινε οραματισμός και ορισμός των διαδικασιών, των χρήσεων και των αποτελεσμάτων των υπηρεσιών ΥΔΚ πριν την υλοποίησή τους. Όπως και σε άλλους τομείς τεχνολογικής προόδου, η υλοποίηση της τεχνολογίας προηγούνταν αλλαγών και διορθωτικών ρυθμίσεων σε διοικητικό, διαδικαστικό και κοινωνικό επίπεδο.

ζ) Κατά την μετάβαση σε περιβάλλον ΥΔΚ, απαιτήθηκε από τους συμμετέχοντες ανώτερο επίπεδο εμπιστοσύνης και επίγνωσης τεχνολογίας. Σε πολλές περιπτώσεις αυτό προκάλεσε εμπόδια, αύξησε το κόστος των λειτουργιών και απαίτησε μεγαλύτερο χρόνο προσαρμογής.

η) Υπήρξαν πολλές περιπτώσεις αποτυχίας στην υιοθέτηση του νέου περιβάλλοντος, είτε σε εύρος χρήσης, είτε σε βάθος χρόνου.

4.1.2 Λογική δομή, ανάλυση και εφαρμογή ΥΔΚ-ΣΥΖΕΥΞΙΣ

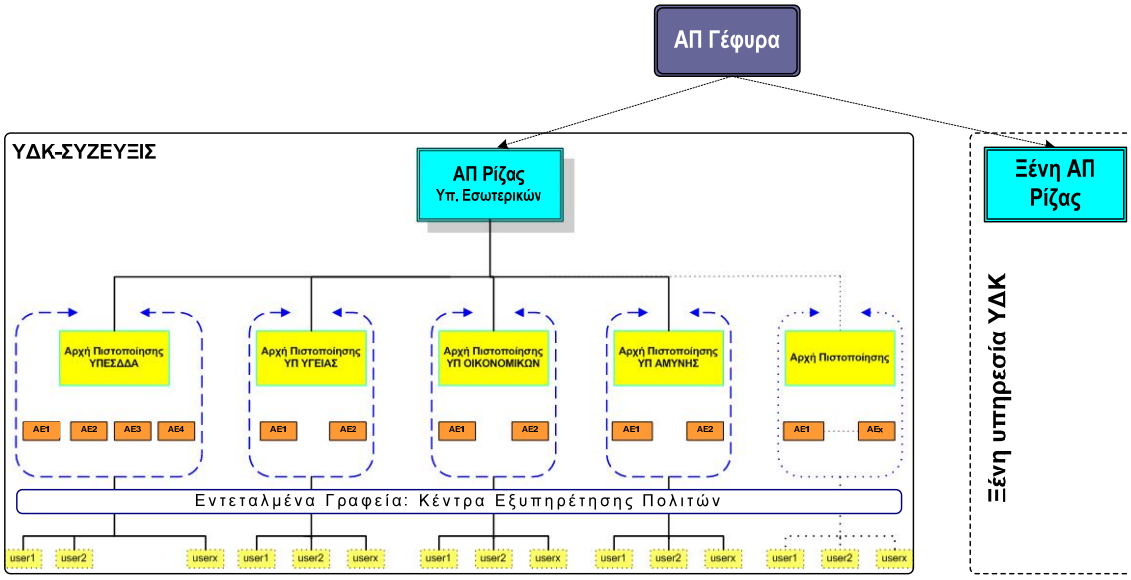
Η ΥΔΚ-ΣΥΖΕΥΞΙΣ υιοθετεί μια διπλή ιδιωτική-δημόσια ιεραρχική δομή. Όλα τα εσωτερικά στο ΣΥΖΕΥΞΙΣ πιστοποιητικά εκδίδονται από την ιδιωτική ιεραρχία (η οποία περιγράφεται παρακάτω), ενώ όλα τα πιστοποιητικά εξυπηρετητών SSL, προσβάσιμα από το Διαδίκτυο, εκδίδονται από την Secure Server Certification Authority της Verisign (νυν Symantec). Το τελευταίο επιλέχθηκε έτσι ώστε τα προγράμματα περιήγησης των χρηστών να εμπιστεύονται σιωπηρά τα πιστοποιητικά των εξυπηρετητών, χωρίς να χρειάζεται δημοσίευσή τους και ρητή δήλωση εμπιστοσύνης σε αυτά. Σαν αποτέλεσμα, για την έκδοση των πιστοποιητικών SSL η ΥΔΚ-ΣΥΖΕΥΞΙΣ περιλαμβάνει μόνο μία ΑΕ.

Για την ιδιωτική ιεραρχία, η ΥΔΚ-ΣΥΖΕΥΞΙΣ καθορίζει μία ΑΠ Ρίζας (Πρωτεύουσα Αρχή Πιστοποίησης – ΠΑΠ) και πολλαπλές υφιστάμενες ΑΠ (Υποκείμενες Αρχές Πιστοποίησης – ΥπΑΠ), οι οποίες και εκδίδουν τα πιστοποιητικά. Η ΠΑΠ βρίσκεται στην αρμοδιότητα της ΑΠΕΔ, ενώ καθεμία από τις ΥπΑΠ (πέντε αρχικά) είναι στην αρμοδιότητα των συμμετεχόντων υπουργείων. Ο προϋπολογισμός αφορούσε μία ΥπΑΠ για κάθε ένα από τα υπουργεία Εσωτερικών, Οικονομικών, Υγείας, Εθνικής Άμυνας και Δημοσίας Τάξης. Εκτός από τις ΑΠ, η ΥΔΚ-ΣΥΖΕΥΞΙΣ καθορίζει ένα αριθμό ΑΕ, έτσι ώστε να μπορεί να εξυπηρετεί μεγάλο αριθμό αιτήσεων πιστοποίησης από τους διάφορους τομείς της ΕΔΔ. Μέσα σε κάθε συμμετέχοντα φορέα, οι ΑΕ κατανέμονται στις κύριες γεωγραφικές περιοχές της χώρας. Συνολικά, η αρχική πρόβλεψη ήταν τέσσερεις ΑΕ για το Υπουργείο Εσωτερικών, δύο ΑΕ για το Υπουργείο Οικονομικών, δύο ΑΕ για το Υπουργείο Υγείας, δύο ΑΕ για το Υπουργείο Άμυνας και μία ΑΕ για το Υπουργείο Δημοσίας Τάξης. Για την κατανομή των ΑΕ ελήφθησαν υπόψη κυρίως ο αριθμός των χρηστών, καθώς και η γεωγραφική κατανομή τους. Τέλος, προϋπολογίστηκε η δυνατότητα διπλασιασμού των ΑΠ και ΑΕ.

Στο τελευταίο και κατώτερο επίπεδο της ιεραρχίας είναι τα Εντεταλμένα Γραφεία (ΕΓ). Το ΕΓ διευκολύνει τις συναλλαγές της ΥΔΚ με τον φυσικό κόσμο, όπως η συλλογή εγγράφων και φορμών, η διανομή των έξυπνων καρτών και η επαλήθευση φυσικής ταυτότητας. Το ρόλο των ΕΓ ορίστηκε να έχουν τα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ), για λόγους κάλυψης ευρείας γεωγραφικής περιοχής.

Η ιεραρχική δομή μιας ΥΔΚ είναι από τη φύση της ιδιαίτερη επεκτάσιμη. Ωστόσο, επειδή η ΥΔΚ-ΣΥΖΕΥΞΙΣ είναι ένα εθνικό σύστημα, σχεδιάστηκε και εξοπλίστηκε ρητά για να επεκτείνεται σε μεγάλο μέγεθος, ώστε να μπορεί να περιλάβει επιπρόσθετες

ΑΠ, ΑΕ και ΕΓ δημοσίων τομέων που θα επιθυμούσαν να συμμετέχουν στο μέλλον. Επιπλέον, είναι δυνατή (και έχει γίνει πρόβλεψη) η σύνδεσή της με ευρωπαϊκές ΥΔΚ (όπως η IDA), μέσω γεφύρωσης. Στο Σχήμα 12 παρουσιάζεται η λογική ιεραρχία ΑΠ Ρίζας-Υφιστάμενη ΑΠ-ΑΕ-ΕΓ της ΥΔΚ-ΣΥΖΕΥΞΙΣ και η δυνατότητα σύνδεσής της μέσω ΑΠ Γέφυρας με εξωτερικές ΥΔΚ.



Σχήμα 12. *Λογική δομή ιεραρχίας ΥΔΚ-ΣΥΖΕΥΞΙΣ.*

4.1.3 Συμμόρφωση με πρότυπα και νομικό πλαίσιο

Από την σύλληψη της η ΥΔΚ-ΣΥΖΕΥΞΙΣ προδιαγράφηκε για να είναι σύμφωνη με τις απαιτήσεις των πιο σημαντικών προτύπων ΥΔΚ, δίνοντας ιδιαίτερη προσοχή σε αυτά που έχουν θεσπιστεί από την Ε.Ε. Ειδικότερα:

α) Προφίλ πιστοποιητικού
   RFC 3739
   ETSI TS 101 862: Qualified Certificate Profile

β) Υπηρεσίες πιστοποίησης
   RFC 3647
   ETSI TS 101 456: Policy requirement for certification authorities issuing qualified certificates
   ANSI X9.79-2001: Financial services public key infrastructure (PKI) policy and practices framework
   AICPA/CICA WebTrust program for certification authorities

γ) Πάροχος υπηρεσιών πιστοποίησης και εγκαταστάσεις
   Common Criteria for Information Technology Security Evaluation (CCITSE), EAL4
   ISO/IEC 17799:2005 και 27001:2005
   AICPA/CICA SAS70 Type II

δ) Κρυπτογραφικός εξοπλισμός
   Information Technology Security Evaluation Criteria (ITSEC) – E3
   CCITSE, EAL4
   FIPS PUB 140-1, Level 3

ε) Έξυπνες κάρτες
   ITSEC – E3
   CCITSE – EAL4+
   ISO/IEC 7816-1-3, ISO/IEC 10373-3, PKCS#11 v2.20

Η συμμόρφωση της υπηρεσίας με τα πρότυπα είναι απαραίτητη προκειμένου να διασφαλιστεί η διαπίστευσή της από την ΕΕΤΤ, καθώς και προς συμμόρφωση με το νομικό της πλαίσιο, όπως αυτό σκιαγραφείται στη συνέχεια. Κυρίως όμως, είναι σημαντική ώστε να ανυψώσει την εμπιστοσύνη των χρηστών προς αυτήν.

Το νομικό πλαίσιο της ΥΔΚ-ΣΥΖΕΥΞΙΣ βασίζεται την οδηγία της ΕΕ 1999/93/ΕC 'On a Community framework for electronic signatures' και σε αριθμό ειδικών νόμων και οδηγιών που έχουν εκδοθεί από την ΕΔΔ (Π.Δ. 150/2001) και την ΕΕΤΤ (248/71/2002, 405/009/27-9-2006, ΦΕΚ 1654/10-11-2006) για την ενσωμάτωση της κοινοτικής οδηγίας στην Ελληνική νομοθεσία. Αυτό το νομικό και κανονιστικό πλαίσιο ακολουθείται στενά στη Δήλωση Πρακτικής Πιστοποίησης (ΔΠΠ) της ΥΔΚ (σκιαγραφείται παρακάτω), έτσι ώστε να παρέχονται αναγνωρισμένες υπηρεσίες πιστοποίησης και οι συναλλαγές που γίνονται με πιστοποιητικά που έχουν εκδοθεί από αυτήν να έχουν νομική ισχύ.

4.1.4 Εκτίμηση περιοριστικών παραγόντων και κινδύνων

Παρότι το έργο της ΥΔΚ-ΣΥΖΕΥΞΙΣ οδηγήθηκε από διεθνείς πρακτικές, εμπειρίες, πρότυπα και τεχνολογική αρτιότητα και διαχειρίστηκε με προσέγγιση προσαρμογής στο περιβάλλον του, υπήρξε σημαντικός αριθμός κινδύνων και περιοριστικών παραγόντων που δυσκόλεψαν τελικά την επιτυχή έκβαση του έργου, την πλατιά υιοθέτησή του και την αποτελεσματικότητά του, ως εξής:

α) Δεν υπήρξε επαρκής πληροφόρηση και συμμετοχή του προσωπικού των υπηρεσιών που συμμετείχαν στην επιχειρησιακή φάση του έργου.
β) Υπήρξαν δυσκολίες, αλλαγές και καθυστερήσεις στην εξεύρεση κατάλληλου προσωπικού και την ανάθεση των καθηκόντων τους στις υπηρεσίες του δημοσίου τομέα στις οποίες ανατέθηκε η διαχείριση της υποδομής και η λειτουργία των ΑΠ, ΑΕ και ΕΓ.
γ) Υπήρξε αοριστία ή αφάνεια στην πρακτική αναγνώριση των υπηρεσιών και των εφαρμογών που θα εξυπηρετούνταν από την ΥΔΚ.
δ) Υπήρξε έλλειψη ευθυγράμμισης με ενέργειες που σχετίζονται με τους τελικούς χρήστες της ΥΔΚ.
ε) Υπήρξαν δυσκολίες στην υιοθέτηση των πρακτικών και των διαδικασιών που προβλέπει η ΥΔΚ από το προσωπικό των οργανισμών του δημοσίου και λανθασμένη θεώρηση της κουλτούρας και των καθιερωμένων πρακτικών των χρηστών.
στ) Υπήρξε υποτίμηση των οργανωτικών, διαδικαστικών, νομικών και κανονιστικών ζητημάτων που πρέπει να αντιμετωπιστούν για την υλοποίηση της ΥΔΚ.

Από την άλλη μεριά, ο σκοπός της διαδικασίας ΑΔ ήταν να βελτιώσει την ασφάλεια της υπηρεσίας ΥΔΚ, όσον αφορά τη χρήση των πιστοποιητικών και τον χειρισμό και διαχείριση των πληροφοριών, προβλέποντας παράγοντες που μπορεί να την απειλήσουν και τοποθετώντας τα κατάλληλα μέτρα ελέγχου για την αντιμετώπισή τους. Το πρότυπο που υιοθετήθηκε και χρησιμοποιήθηκε στην ΥΔΚ-ΣΥΖΕΥΞΙΣ ήταν το ISO/IEC 17799:2005/27001:2005, σε συνδυασμό με ότι πληροφορία για τους χρήστες του συστήματος ήταν διαθέσιμη ή μπορούσε να βρεθεί. Επιπλέον, η διαδικασία ακολούθησε τυπική μεθοδολογία, που συμπεριλάμβανε σειρά βημάτων, όπως απαιτείται από το πρότυπο: α) καθορισμός και ανάλυση της υπηρεσίας ΥΔΚ, β) αναγνώριση των επιβλαβών καταστάσεων, γ) ορισμός ελέγχων και εκτίμηση αυτών, δ) αναγνώριση και κατηγοριοποίηση αδυναμιών, ε) επιλογή αντιμέτρων και στ) σύνταξη αναφορών και συστάσεων.

4.1.5 Δήλωσης πρακτικής πιστοποίησης

Η Δήλωση Πρακτικής Πιστοποίησης (ΔΠΠ) αποτελεί διακήρυξη των πρακτικών που εφαρμόζει μια ΑΠ για τη διαχείριση των πιστοποιητικών που εκδίδει. Περιγράφει πως η Πολιτική Πιστοποίησης (ΠΠ), η οποία επίσης δηλώνεται, μεταφράζεται στο πλαίσιο της αρχιτεκτονικής συστήματος και των λειτουργικών διαδικασιών των οργανισμών

που αφορά. Η ΔΠΠ είναι δεσμευτική για την ΑΠ, αλλά και για τους χρήστες της υπηρεσίας, διαμορφώνει δε τη βάση για τη δημιουργία εμπιστοσύνης μεταξύ τους.

Παρόλο που δεν υπάρχει πρότυπη ΔΠΠ διεθνώς, έχει διαμορφωθεί ένα πλαίσιο το οποίο περιλαμβάνει μια λίστα ελέγχου στοιχείων πολιτικής που πρέπει να περιλαμβάνει. Όλα τα κύρια στοιχεία του πλαισίου εκτιμήθηκαν και συμπεριλήφθησαν στη ΔΠΠ της ΥΔΚ-ΣΥΖΕΥΞΙΣ, βάση του 'X.509 PKI CP and Certification Practices Framework', το Verisign CPS v3.1 και το ελληνικό νομικό/κανονιστικό πλαίσιο που προαναφέρθηκε. Η ΔΠΠ δημοσιεύεται στην ιστοσελίδα της ΥΔΚ-ΣΥΖΕΥΞΙΣ, ώστε να προσβάσιμη από όλους τους χρήστες. Επιπλέον, η ΔΠΠ έχει διαμορφωθεί ειδικά για την οργανωτική δομή, της λειτουργικές διαδικασίες, τις εγκαταστάσεις και το υπολογιστικό περιβάλλον των τομέων της ΕΔΔ που αποτελούν τις αρχές της ΥΔΚ (ΑΠ, ΑΕ και ΕΓ). Χρησιμοποιήθηκε επιπλέον τυπική δομή για την ΠΠ και την υποκείμενη ΔΠΠ, κάτι που βοηθά να διασφαλιστεί η πληρότητά της και να απλοποιηθεί η εκτίμηση του βαθμού διαβεβαίωσης των χρηστών.

Τα κύρια σημεία της ΔΠΠ ΥΔΚ-ΣΥΖΕΥΞΙΣ είναι τα ακόλουθα:

α) *Πεδίο εφαρμογής*: ο αριθμός των ΑΠ και ΑΕ, τα πρότυπα συμμόρφωσης των εξωτερικών διεπαφών, η μορφή των ονομάτων στα πιστοποιητικά, το πεδίο ονομάτων εντός του οποίου σκοπεύουν οι ΑΠ να εκδίδουν πιστοποιητικά.

β) *Ταυτοποίηση και επαλήθευση ταυτότητας*: οι μηχανισμοί που χρησιμοποιούνται για την επαλήθευση της ταυτότητας των συμμετεχόντων στην υπηρεσία, συμπεριλαμβανομένων των χρηστών, του αξιωματικού ασφάλειας, του διαχειριστή ασφάλειας, του διαχειριστή καταλόγου, των αξιωματικών των ΑΕ και μια δήλωση των προνομίων και των ευθυνών που ανατίθενται σε κάθε ρόλο.

γ) *Διαχείριση κλειδιών*: περιγράφεται η διαχείριση του κύκλου ζωής των κλειδιών όλων των δομοστοιχείων της ΥΔΚ (ΑΠ, ΑΕ και χρήστες). Επιπλέον σημεία συμπεριλαμβάνουν την επιλογή του αλγόριθμου ψηφιακής υπογραφής στα πιστοποιητικά, το χρόνο εγκυρότητας των πιστοποιητικών και τον αλγόριθμο για την ψηφιακή υπογραφή δεδομένων.

δ) *Πρακτικές λειτουργίας*: περιγράφονται οι λειτουργικές διαδικασίες των ΑΠ, ΑΕ και των τελικών οντοτήτων, συμπεριλαμβανομένων θεμάτων όπως: εγγραφή μοναδικών ονομάτων, διαγραφή/ανάκληση/ανανέωση πιστοποιητικών, απώλεια κλειδιών, εκδίωξη από αιτία, ανάκτηση ιδιωτικού κλειδιού, έλεγχοι ασφάλειας, πρακτικές auditing, καταγραφή συμβάντων, αρχειοθέτηση, προστασία προσωπι-

κών στοιχείων, αναθεώρηση και ενημέρωση ΠΠ και σχέδιο ανάκαμψης από καταστροφή.

ε) *Προφίλ πιστοποιητικών και Λίστας Ανακληθέντων*: περιγράφονται το περίγραμμα των πιστοποιητικών, ο κατάλογος ανακληθέντων πιστοποιητικών (ΚΑΠ) και το σχήμα του καταλόγου, δείχνοντας ποιες επεκτάσεις πιστοποιητικών και ΚΑΠ είναι παρούσες, εάν αυτές χαρακτηρίζονται κρίσιμες ή μη κρίσιμες, ποια προαιρετικά πεδία υπάρχουν, ποιο είναι το εύρος τιμών που επιτρέπεται και τι πράξεις αναμένονται από τους ελέγχοντες σε απόκριση μη προτύπων επεκτάσεων.

στ) *Τοπικές πρακτικές ασφάλειας*: περιγράφονται πρακτικές ασφάλειας σχετικές με το περιβάλλον στο οποίο λειτουργούν τα κύρια δομοστοιχεία της ΥΔΚ-ΣΥΖΕΥΞΙΣ, συμπεριλαμβανομένων φυσικών ελέγχων, ελέγχων προσωπικού και διαδικαστικών/τεχνικών ελέγχων.

ζ) *Νομικές προβλέψεις*: ορίζονται ρητά οι κανονισμοί στους οποίους πρέπει να συμμορφώνεται η ΥΔΚ-ΣΥΖΕΥΞΙΣ, συμπεριλαμβανομένων αυτών για προστασία δεδομένων, ιδιωτικότητας, πρόσβασης στην πληροφορία και νομοθεσίας νόμιμης παρακολούθησης. Συμπεριλαμβάνονται επίσης η νομική ευθύνη της ΑΠ, οι υποχρεώσεις των ΑΠ και ΑΕ, οι υποχρεώσεις των κατόχων πιστοποιητικών, οι υποχρεώσεις των αξιωματούχων, η αποδοχή περιορισμών και ενημερωμένης αποδοχής. Περιλαμβάνονται επίσης οι συμβάσεις των χρηστών και τρίτων προσώπων και νομικά θέματα που καλύπτονται από αυτές.

η) *Πληροφορία οικονομικής ευθύνης και χρεώσεων*

Μετά από τη σύνταξή της, η ΔΠΠ επανεκτιμήθηκε και κρίθηκε ως επαρκώς αναλυτική και πλήρης. Αποφασίστηκε ότι το κυριότερο μειονέκτημά της είναι ότι, αποτελώντας μέρος ενός πρωτοποριακού για την ΕΔΔ έργου, έχει αποκλειστικά «συμβουλευτικό χαρακτήρα» και δεν είναι δεσμεύει νομικά τις συμμετέχουσες οντότητες. Οι αρχές που ορίζονται για την υλοποίησή της δεν μπορούν να υποχρεωθούν νομικά να ακολουθήσουν τις προβλέψεις της. Έτσι, σχεδιάστηκε και υλοποιήθηκε ένας αριθμός από «μαλακούς» μηχανισμούς και μέτρα ώστε να διασφαλιστεί η εφαρμογή της ΔΠΠ.

Πρώτον, ξεκίνησε μια διαδικασία διαβούλευσης για την οριστικοποίηση και προώθηση της ΔΠΠ ΥΔΚ-ΣΥΖΕΥΞΙΣ, με τη συμμετοχή των ορισμένων ως ΑΠ και ΑΕ φορέων. Δεύτερον, εντός του ευρύτερου έργου ΣΥΖΕΥΞΙΣ, υλοποιήθηκε υποέργο εκπαίδευσης, επίγνωσης και ενδυνάμωσης ανθρωπίνων πόρων, ώστε να αντιμετωπιστούν και να προωθηθούν οι οργανωτικές και διοικητικές αλλαγές που απαιτούνται από την ΥΔΚ.

Εντός αυτού του υποέργου, συμπεριελήφθησαν ειδικά θέματα τεχνολογίας και διοίκησης ΥΔΚ. Επιπλέον, σχεδιάστηκαν και παραδόθηκαν ειδικά μαθήματα και για τα τρία επίπεδα (ΑΠ, ΑΕ και ΕΓ) του προσωπικού της ΕΔΔ που ενέχονταν, των οποίων το περιεχόμενο αφορούσε τις τεχνικές, διοικητικές και νομικές απόψεις της διαχείρισης πληροφορίας, ασφάλειας και βέλτιστων πρακτικών ΥΔΚ, για πολλαπλά προφίλ εκπαιδευόμενων.

Τέλος, ξεκίνησε διαδικασία νομοθέτησης δεσμευτικού νομικού πλαισίου, μέσω σχετικού προεδρικού διατάγματος, που ανέθεσε τον ρόλο της Αρχής της ΥΔΚ σε συγκεκριμένη υπηρεσία του Υπουργείου Εσωτερικών και επέβαλε την τήρηση της ΔΠΠ σε όλα τα μέρη που συμμετέχουν.

4.1.6 Εφαρμογή της μεθοδολογίας ΑΔ στην ΥΔΚ-ΣΥΖΕΥΞΙΣ

Από τα παραπάνω, αλλά και από τελικά αποτελέσματα, την αποδοχή και την επιτυχία του έργου της ΥΔΚ-ΣΥΖΕΥΞΙΣ, είναι φανερό ότι και σε αυτή την περίπτωση η διαδικασία ΑΔ που χρησιμοποιήθηκε δεν κάλυψε σημαντικές απόψεις των κινδύνων που αντιμετώπισε το έργο. Η διαδικασία κάλυψε μεν ικανοποιητικά τους τεχνικούς κινδύνους για τη λειτουργία του έργου και τη διασφάλιση των πληροφοριών των χρηστών του και πρότεινε κατάλληλα αντίμετρα για την ανύψωση της ασφάλειας της υπηρεσίας. Ωστόσο, από το (αρνητικό) αποτέλεσμα κρίνεται ότι, όσον αφορά την ολότητα του έργου και την επιτυχία των στόχων του, δεν έγινε σωστή εκτίμηση (στη πραγματικότητα δεν έγινε καθόλου) σημαντικών κινδύνων, οι οποίοι αφορούσαν περιοχές όπως η πολιτική ηγεσία, το διοικητικό προσωπικό των εμπλεκομένων υπηρεσιών, αλλά κυρίως των ατόμων που στοχεύονταν ως χρήστες της υπηρεσίας. Γι' αυτούς τους κινδύνους δεν υιοθετήθηκαν τα κατάλληλα μέτρα και τελικά το έργο δεν πέτυχε τη διείσδυση και την αποδοχή, σε πλάτος χώρου και βάθος χρόνου, που φιλοδοξούσε. Υπήρξαν και κάποια προβλήματα με τους οδηγούς και την υποστήριξη των έξυπνων καρτών που διανεμήθηκαν, αλλά κατά τη γνώμη του συγγραφέα (ο οποίος συμμετείχε στην ομάδα ανάπτυξης του έργου), αυτό δεν επηρέασε το τελικό αποτέλεσμα.

Στο σημείο αυτό θα γίνει σύντομη εφαρμογή της προτεινόμενης μεθοδολογίας στην ΥΔΚ-ΣΥΖΕΥΞΙΣ. Στον Πίνακα 4 του Παραρτήματος Α αναπτύσσεται η μήτρα RIPC[4] για το επίπεδο κινδύνων τελικού χρήστη. Σε αυτό το παράδειγμα υπολογίζεται τελικά ότι:

$Ri = 0,42$ $Ci = 0,87$

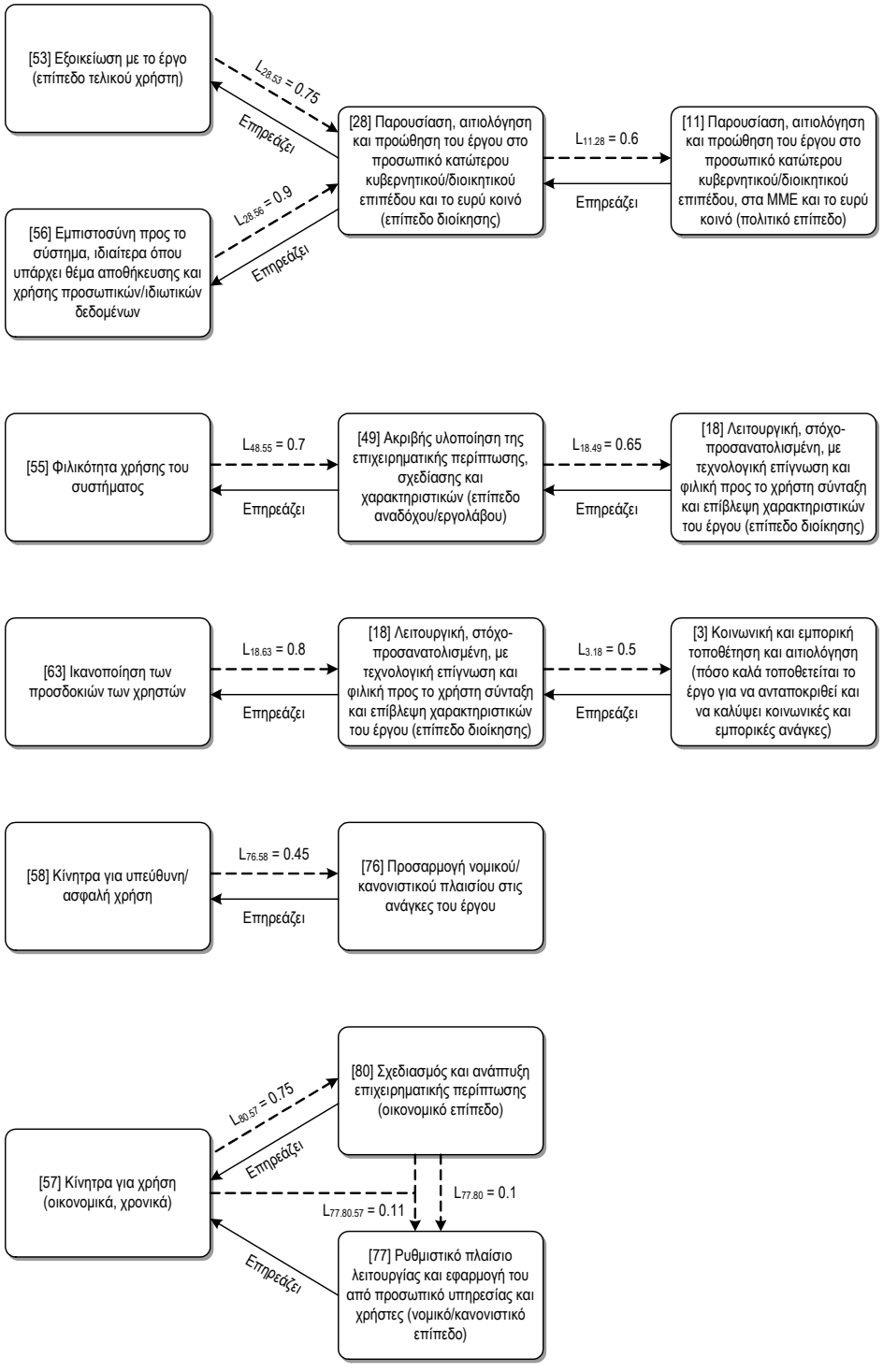
$Co = 76$ $Mi = 0,153$

Ερμηνεύοντας τους δείκτες, συμπεραίνεται ότι ο κίνδυνος είναι αρκετά υψηλός στο προκείμενο απόσπασμα εφαρμογής στην περιοχή κινδύνων τελικού χρήστη, διότι η εκτίμηση κάλυψης των αντιμέτρων δεν ακολουθεί στενά την επίπτωση. Αυτό φαίνεται τόσο από την τιμή του *Ci* (που δείχνει χαμηλή κάλυψη) όσο και από τη μικρή τιμή του *Mi* (προσέγγιση κάλυψης στο κατώφλι). Από την άλλη μεριά, το κόστος των αντιμέτρων είναι σχετικά χαμηλό.

Το συμπέρασμα (ακόμα και αυτής της περιορισμένης εφαρμογής) της προτεινόμενης μεθοδολογίας ΑΔ ταιριάζει με την περιορισμένη διείσδυση του έργου. Αυτό διότι, ενώ το έργο ήταν καλομελετημένο και η υλοποίησή του από τον ανάδοχο σχεδόν χωρίς ελαττώματα, υπήρξαν σημαντικοί περιοριστικοί παράγοντες για τη λειτουργία του, όπως η περιορισμένη υποστήριξη στο πολιτικό και διοικητικό επίπεδο. Κυρίως όμως το πρόβλημα εντοπιζόταν στην περιορισμένη τεχνογνωσία ανάπτυξης σχετικών ΥΔΚ- ενεργοποιημένων εφαρμογών στους φορείς-πελάτες, τόσο από το προσωπικό των φορέων υλοποίησης, όσο και από τους αναδόχους των υπό υλοποίηση έργων. Ο βασικός λόγος λοιπόν της περιορισμένης επιτυχίας της ΥΔΚ-ΣΥΖΕΥΞΙΣ (ο οποίος αντανακλάται στην εφαρμογή της προτεινόμενης μεθοδολογίας ΑΔ στον αντίστοιχο κίνδυνο και στην κάλυψή του) ήταν ότι οι στοχευόμενοι χρήστες – δημόσιοι υπάλληλοι δεν είχαν στη διάθεσή τους χρήσιμες εφαρμογές (=κίνητρα) για την χρήση των πιστοποιητικών. Αντίθετα, αν εξαιρεθεί η περιορισμένη τεχνική υποστήριξη των έξυπνων καρτών, η υπόλοιπη εμπειρία τους, πχ. όσον αφορά την προμήθεια πιστοποιητικών και έξυπνων καρτών, ήταν ικανοποιητική.

Τα αντίμετρα που προτείνει η μεθοδολογία για την μείωση της επικινδυνότητας του συγκεκριμένου κινδύνου (κίνητρα χρήσης) είναι: α) Εύκολη πρόσβαση σε ηλεκτρονικές υπηρεσίες που μειώνουν την ανάγκη για φυσική παρουσία, β) μικρότερες διαχειριστικές απαιτήσεις, γ) πρόσβαση σε προωθημένες υπηρεσίες αν χρησιμοποιηθεί το σύστημα (πχ. έξυπνες κάρτες και υποδομή ΥΔΚ), δ) μελέτη σκοπιμότητας και επιχειρηματική τοποθέτηση του έργου ώστε να ανταποκρίνεται σε πραγματικές ανάγκες των ενδιαφερόμενων φορέων, ομάδων, χρηστών, ε) εκστρατεία δημιουργίας κινήτρων και αναγκών στους χρήστες (εφόσον οι πραγματικές δεν επαρκούν/υπάρχουν). Είναι φανερό ότι αν είχαν ληφθεί αυτά τα μέτρα (τα οποία συμπεριλαμβάνουν τη δημιουργία χρησίμων εφαρμογών βασιζομένων στην ΥΔΚ), η διείσδυση της ΥΔΚ-ΣΥΖΕΥΞΙΣ θα ήταν πολύ μεγαλύτερη.

Συνεχίζοντας την εφαρμογή της προτεινόμενης μεθοδολογίας στην ΥΔΚ-ΣΥΖΕΥΞΙΣ, θα ληφθούν υπόψη και οι εξαρτήσεις μεταξύ των κινδύνων στον υπολογισμό της διακινδύνευσης. Το Σχήμα 13 εικονίζει απόσπασμα του γράφου αλληλεξάρτησης κινδύνων για το επίπεδο κινδύνων τελικού χρήστη, με τις εξαρτήσεις και τα ενδεχόμενα αντίστροφης πραγμάτωσης.



Σχήμα 13. *Παράδειγμα υπολογισμού γράφου αλληλεξάρτησης κινδύνων*

Στον Πίνακα 5 του Παραρτήματος Α παρουσιάζεται η νέα διαμόρφωση της μήτρας RIPC[4], με τις νέες (μετέπειτα) πιθανότητες πραγμάτωσης των κινδύνων να φαίνονται στη στήλη P_{post}, ενώ η αρχική στήλη Πιθανότητα μετονομάστηκε σε P_{pri}. Στη μήτρα συμπεριλαμβάνονται και κίνδυνοι από άλλα επίπεδα, από τους οποίους εξαρτώνται οι κίνδυνοι επιπέδου τελικού χρήστη. Γι' αυτούς έχουν, για λόγους συντομίας, συμπληρωθεί μόνο οι απαραίτητες για τους υπολογισμούς πρότερες πιθανότητες P_{pri}.

Σε αυτό το παράδειγμα, μπορούμε να δούμε ότι η πιθανότητα των κινδύνων 55, 56, 57 και 63 έχει αυξηθεί σημαντικά, λόγω διαδοχικής εξάρτησης από άλλους κινδύνους με σχετικά υψηλές πιθανότητες. Επισημαίνονται ιδιαίτερα ο κίνδυνος 63 "ικανοποίηση των προσδοκιών των χρηστών" και ο κίνδυνος 56 «εμπιστοσύνη προς το σύστημα, ιδιαίτερα όπου υπάρχει θέμα αποθήκευσης και χρήσης προσωπικών/ιδιωτικών δεδομένων», κάτι που απεικονίζει την αυξημένη σημαντικότητα των αντιμέτρων γι' αυτούς τους κινδύνους, όπως και την χρησιμότητα αυτής της επέκτασης στη μεθοδολογία μας.

Με αυτόν τον υπολογισμό, ο δείκτης *Ri* παίρνει τη νέα τιμή 0,43, το οποίο δείχνει ότι η συνολική διακινδύνευση αυξήθηκε ελαφρά, λόγω του ότι ελήφθεισαν υπόψη οι εξαρτήσεις μεταξύ των κινδύνων.

4.2 Εφαρμογή σε πρωτότυπη ΥΔΚ

4.2.1 Γενική περιγραφή ΥΔΚ που προστατεύει το ιδιοαπόρρητο και την ελευθερία βούλησης

Σε αυτό το σημείο, περιγράφουμε μια πρωτότυπη ΥΔΚ που προστατεύει το απόρρητο προσωπικών πληροφοριών (ιδιοαπόρρητο) και την ελευθερία βούλησης των χρηστών της. Η αρχική επιδίωξη ήταν να αποτελέσει μια παραδειγματική περίπτωση εφαρμογής της προτεινόμενης μεθοδολογίας, διαθέτοντας όλα τα «επικίνδυνα» χαρακτηριστικά που πραγματεύεται. Όμως ο πρωτότυπος τρόπος αντιμετώπισης της προστασίας του ιδιοαπόρρητου που εισάγει, οδήγησε σε μια υποδειγματική καθεαυτό ΥΔΚ, η οποία προτάθηκε για δημοσίευση (Kefallinos & Sykas, 2012).

Εν συντομία, πρόκειται για μια υβριδική ΥΔΚ πιστοποιητικών ταυτότητας (ΠΤ) και πιστοποιητικών χαρακτηριστικών (ΠΧ), με χαρακτηριστικά ανωνυμίας που βασίζονται σε ψευδώνυμα. Στόχοι της είναι: α) να αντιμετωπίσει τις ανησυχίες για παρακολούθηση των κινήσεων/συναλλαγών των χρηστών των ΥΔΚ, δυσχεραίνοντάς την, β) να υπερασπιστεί το απόρρητο των προσωπικών στοιχείων των χρηστών και γ) να διαφυλάξει την ελευθερία βούλησής τους. Αυτά προσφέροντας χωρίς περιορισμούς υπηρεσίες πιστο-

ποίησης ταυτότητας και χαρακτηριστικών, για εφαρμογές επαλήθευσης ταυτότητας, εξουσιοδότησης και ψηφιακών υπογραφών, βασιζόμενη σε πρότυπα πιστοποιητικά/αλγόριθμους και εμπορικά συστήματα ΥΔΚ.

Τα πιστοποιητικά ταυτότητας (ΠΤ – identity certificates – IDC) ή πιστοποιητικά δημοσίου κλειδιού (public key certificates – PKC) και οι αντίστοιχες Υποδομές Δημοσίου Κλειδιού (ΥΔΚ) θεωρούνται η καλύτερη λύση για την ολοκλήρωση υπηρεσιών επαλήθευσης ταυτότητας και ψηφιακής υπογραφής στις περισσότερες σύγχρονες εφαρμογές που αναπτύσσονται, τόσο για το Διαδίκτυο, όσο και για επιχειρησιακά δίκτυα. Ωστόσο, οι νέες εφαρμογές εμπορικών ή κυβερνητικών ηλεκτρονικών επιγραμμικών (online) συναλλαγών, χρειάζονται και υπηρεσίες εξουσιοδότησης πρόσβασης (authorization) προκειμένου να οριστούν κατηγορίες χρηστών με διαφορετικά προνόμια και να αντιστοιχιστούν σε εσωτερικούς λογαριασμούς χρηστών.

Καθώς τα απλά διαπιστευτήρια (simple credentials) δεν είναι ούτε επαρκή ούτε ασφαλή για την συσχέτιση ενός χρήστη με τον εσωτερικό στον οργανισμό αποδέκτη (ΟΑ) λογαριασμό του (internal user account), ορίζεται τυπικά ένα χαρακτηριστικό ταυτοποίησης Ειδικό για τον Οργανισμό Αναγνωριστικό (ΕΟΑ), το οποίο αναγνωρίζει μοναδικά το άτομο εντός του πεδίου της εσωτερικής βάσης δεδομένων του ΟΑ. Για εφαρμογές εξουσιοδότησης, συνδέει την συνεδρία του χρήστη με τον εσωτερικό λογαριασμό και αναθέτει δικαιώματα. Για εφαρμογές ηλεκτρονικής υπογραφής, συσχετίζει τα ψηφιακά υπογεγραμμένα δεδομένα (συναλλαγές, έγγραφα κτλ) με τον εσωτερικό λογαριασμό για σκοπούς αποφυγής αποκήρυξης ευθύνης (non-repudiation).

Έχουν προταθεί διάφορες λύσεις στο παρελθόν για την αντιμετώπιση του προβλήματος. Για παράδειγμα, στη σύσταση X.509 (ITU-T, 2005, 2008) η ITU-T έχει προτείνει πιστοποιητικά χαρακτηριστικών (ΠΧ), τα οποία αποτελούν τη βάση για να δημιουργηθεί μια Υποδομή Διαχείρισης Προνομίων (ΥΔΠ). Τα ΠΧ περιέχουν την πληροφορία που χρειάζεται στο πεδίο Attributes, χωρίς την παρουσία δημόσιου κλειδιού του κατόχου τους.

Εδώ όμως εμφανίζεται το πρόβλημα του προσωπικού απορρήτου. Όπως ορίζεται από τον Westin (1967), το προσωπικό απόρρητο (ή ιδιοαπόρρητο) της πληροφορίας (personal information privacy) είναι η απαίτηση ατόμων, ομάδων ή οργανισμών να αποφασίζουν οι ίδιοι πότε, πως και μέχρι ποιο βαθμό θα απελευθερωθούν πληροφορίες που τους αφορούν σε τρίτους. Η διασύνδεση των πληροφοριακών συστημάτων των δημόσιων και ιδιωτικών οργανισμών, σε συνδυασμό με τη μεγάλη ανάπτυξη του εμπορίου της πληροφορίας, εντείνει το πρόβλημα της διάχυσης των ιδιωτικών στοιχείων των α-

τόμων, πέρα και πάνω από τον έλεγχό τους. Τα αποτελέσματα μπορεί να είναι πολύ μεγαλύτερα από την απλή όχληση λόγω συνεχούς βομβαρδισμού με προσφορές και διαφημιστικά μηνύματα και μπορεί να συνοψισθεί στη δημιουργία κατατομών συνηθειών, προτιμήσεων, συμπεριφορών, κινήσεων και χαρακτηριστικών των ατόμων, με σκοπούς που κυμαίνονται από την απλή στοχευμένη προώθηση προϊόντων, μέχρι την πρόβλεψη ενεργειών και την παρακολούθηση της ζωής τους, με τελικό αποτέλεσμα την καταστρατήγηση της ελευθερίας της βούλησης και των πράξεων.

Όσον αφορά τις ΥΔΚ, είναι γενικά παραδεκτό πως αν ποτέ ευοδωθούν οι οραματισμοί για διασύνδεση όλων των τοπικών, εθνικών και διεθνών ΥΔΚ, τότε η συστηματική συσχέτιση και παρακολούθηση των πράξεων και συναλλαγών των ιδιοκτητών πιστοποιητικών θα είναι πολύ εύκολη και όλοι θα υποχρεωθούν να επικοινωνούν και να συναλλάσσονται εντός του πιο καθολικού συστήματος ηλεκτρονικής παρακολούθησης που φτιάχτηκε ποτέ (Brands, 1999).

Το κίνητρο λοιπόν για την ανάπτυξη της προτεινόμενης ΥΔΚ ήταν η πεποίθηση του συγγραφέα ότι η έρευνα και ανάπτυξη που έγινε στο παρελθόν σε αυτό τον τομέα είναι είτε πολύ περιοριστική, είτε πολύ ειδικευμένη, είτε πολύ δύσκολη στην υλοποίηση, είτε ένας συνδυασμός των παραπάνω. Επιπλέον, οι ΥΔΚ που έχουν αναπτυχθεί στις περισσότερες χώρες, τόσο ιδιωτικές όσο και δημόσιες, δεν προστατεύουν, κατά την άποψή του, το απόρρητο προσωπικών δεδομένων. Μάλιστα, δεν έχει μέχρι σήμερα υπάρξει υλοποίηση μεγάλου μεγέθους εθνικής ή ιδιωτικής ΥΔΚ με στοιχεία ανωνυμίας και προστασίας των προσωπικών δεδομένων. Σε ΥΔΚ της Β. Αμερικής, Ευρώπης, Ασίας και Αυστραλίας που ερευνήθηκαν, στις περιπτώσεις που απαιτούνταν η ύπαρξη χαρακτηριστικών των χρηστών για σκοπούς ταυτοποίησης, εξουσιοδότησης ή αποφυγής αποκήρυξης ευθύνης, ακολουθήθηκε η απλή μέθοδος του να συμπεριληφθούν εντός των ΠΤ, με χρήση πολλαπλών κατατομών πιστοποιητικών και ΠΠ, όπου χρειαζόταν. Αυτό, παρότι είναι λειτουργικό, δεν προάγει ακριβώς την προστασία προσωπικών δεδομένων.

Αντίθετα στην πρότασή μας, καταβλήθηκε προσπάθεια να εξευρεθεί ένα μοντέλο που θα ακολουθεί τα πρότυπα, θα είναι εύκολο στην υλοποίηση, θα απαιτεί όσο λιγότερη ανάπτυξη λογισμικού είναι δυνατόν για να ενσωματωθεί εντός εμπορικών ΥΔΚ, θα είναι κατάλληλο για χρήση σε μεγάλη κλίμακα και θα παραχωρεί λίγα στην προστασία των προσωπικών δεδομένων.

Πιο λεπτομερώς, το μοντέλο πρέπει να ακολουθεί τις ακόλουθες αρχές, παραμέτρους, περιορισμούς και απαιτήσεις:

α) Πρέπει να μπορεί να χρησιμοποιηθεί σε μια (εθνική) ΥΔΚ μεγάλης κλίμακας.

β) Πρέπει να προωθεί μια ενοποιημένη αρχιτεκτονική πιστοποίησης, που θα περιλαμβάνει καθολική Ασφαλή Διάταξη Αποθήκευσης Πιστοποιητικών (ΑΔΑΠ) (έξυπνη κάρτα ή αδειοδοτικό USB) για εφαρμογές τόσο του δημόσιου όσο και του ιδιωτικού τομέα.

γ) Πρέπει να προστατεύει τα προσωπικά δεδομένα του ατόμου, όπως πχ. ΑΦΜ, ΑΔΤ, ΑΜΚΑ.

δ) Πρέπει να διασφαλίζει ότι δεδομένα μη απαραίτητα για μια συναλλαγή δεν ελευθερώνονται στον αποδέκτη της και σε τρίτους.

ε) Πρέπει να δυσχεραίνει την καθιέρωση καθολικού αναγνωριστικού ταυτοποίησης (ΚΑΤ) πολιτών και διασφαλίζει ότι δεν δίδονται κίνητρα για την υιοθέτηση από έναν οργανισμό χαρακτηριστικού ταυτοποίησης που αφορά έναν άλλο.

στ) Πρέπει να προασπίζει την ελευθερία βούλησης του κοινού. Κανείς δεν θα πρέπει να υποχρεώνεται στο να παρέχει μη απαραίτητα προσωπικά στοιχεία σε ένα οργανισμό προκειμένου να διεξάγει συναλλαγές με αυτόν και θα μπορεί να αποκαλύπτει τα ελάχιστα απαιτούμενα για την ολοκλήρωση μιας συναλλαγής. Η (συχνά εκβιαστική) υποχρέωση να αποκαλύπτονται περισσότερα πρέπει να αποκρούεται.

ζ) Τα ΠΤ που εκδίδονται δεν πρέπει να είναι ανώνυμα και δεν πρέπει να εκδίδονται από τους ΟΑ που υλοποιούν τις εφαρμογές που δέχονται και ελέγχουν την εγκυρότητα τους.

η) Δεν πρέπει να υποχρεώνει έναν ΟΑ να υιοθετεί το μοντέλο εμπιστοσύνης ‘trust the root’. Ο ΟΑ πρέπει να μπορεί να επιλέγει ποια πιστοποιητικά αποδέχεται.

θ) Το σύστημα θα πρέπει να βασίζεται σε εμπορικούς αλγόριθμους συμμετρικής και ασύμμετρης κρυπτογράφησης και Χ.509 ΠΤ και ΠΧ, ώστε να είναι δυνατή η εύκολη υλοποίησή του.

ι) Θα πρέπει να παρέχεται τεχνικός τρόπος για την αποτελεσματική αντιστοίχηση του σειριακού αριθμού ενός ΠΤ με ένα ΕΟΑ. Αυτή αποτελεί πρωτεύουσα απαίτηση για τη σχεδίαση του συστήματος, διότι:

   i) Ο απλός συνδυασμός ονόματος-επωνύμου που περιέχεται σε ένα ΠΤ δεν επαρκεί για την αποτελεσματική ταυτοποίηση του υποκειμένου,

   ii) Είναι απαραίτητη η υποστήριξη πολλαπλών ΟΑ και

   iii) Δεν μπορεί και δεν πρέπει να επιτευχθεί η παρακολούθηση του ιδιοκτήτη του μέσω του σειριακού αριθμού του ΠΤ, καθώς αυτό προσκρούει στην προηγούμενη απαίτηση περί αποφυγής καθιέρωσης ΚΑΤ.

Το ΕΟΑ πρέπει να είναι μοναδικό για κάθε ΟΑ και το σύστημα πρέπει να περιλαμβάνει μηχανισμούς – δικλείδες ασφαλείας, ώστε να προφυλάσσει από τον επιμερισμό και τη διάχυση των ΕΟΑ μεταξύ των ΟΑ και να αποφευχθεί η *de facto* καθιέρωση ΚΑΤ.

4.2.2 Αναλυτική περιγραφή του προτεινόμενου μοντέλου ΥΔΚ

Στο προτεινόμενο μοντέλο ΥΔΚ, οι οντότητες που μετέχουν είναι: α) οι χρήστες - ιδιοκτήτες των πιστοποιητικών, β) μία ή περισσότερες ΑΠ, γ) μία ή περισσότερες Αρχές Εξουσιοδότησης (ΑΕξ), δ) μια Έμπιστη Τρίτη Αρχή (ΕΤΑ) και ένας ή περισσότεροι ΟΑ. Οι ΑΠ εκδίδουν τυπικά X.509v3 ΠΤ, οι ΑΕ εκδίδουν X.509/RFC5755 ΠΧ που περιέχουν τα απαιτούμενα χαρακτηριστικά (ΕΟΑ), η ΕΤΑ διατηρεί τις συσχετίσεις ψευδωνύμων/ταυτοτήτων και οι ΟΑ εκδίδουν τα ΕΟΑ που τους αφορούν και αποδέχονται τα ΠΧ που επιθυμούν (ελέγχοντας το πεδίο 'Issued by'). Οι χρήστες διαθέτουν ασφαλείς διατάξεις αποθήκευσης πιστοποιητικών (ΑΔΑΠ), τουλάχιστον FIPS 140-2 Level 2 επιπέδου (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf). Το μοντέλο είναι ένας συνδυασμός συμβατικής υποδομής με γένεια X.509 ΠΤ και υβριδικής ΠΤ-ΠΧ υποδομής με χρήση ψευδωνύμων ΠΧ.

Στα πλαίσια του μοντέλου, ένας χρήστης εγγράφεται σε έναν ή περισσότερους ΟΑ που υλοποιούν τις εφαρμογές που επιθυμεί να χρησιμοποιήσει. Η εγγραφή τυπικά ενέχει τη δημιουργία ενός εσωτερικού στο πληροφοριακό σύστημα του ΟΑ λογαριασμού, που αναθέτει στον χρήση ένα ΕΟΑ και απλά διαπιστευτήρια τύπου όνομα χρήστη – κωδικός. Λαμβάνεται ως δεδομένο ότι αυτά τα απλά διαπιστευτήρια δεν αποτελούν απόδειξη ταυτότητας ή κατοχής του ΕΟΑ. Ως αποτέλεσμα δεν είναι υποχρεωτική η ύπαρξή τους, βοηθούν όμως στη δημιουργία της συνεδρίας του χρήστη με την εφαρμογή πλευράς εξυπηρετητή (ΕΠΕ) του ΟΑ.

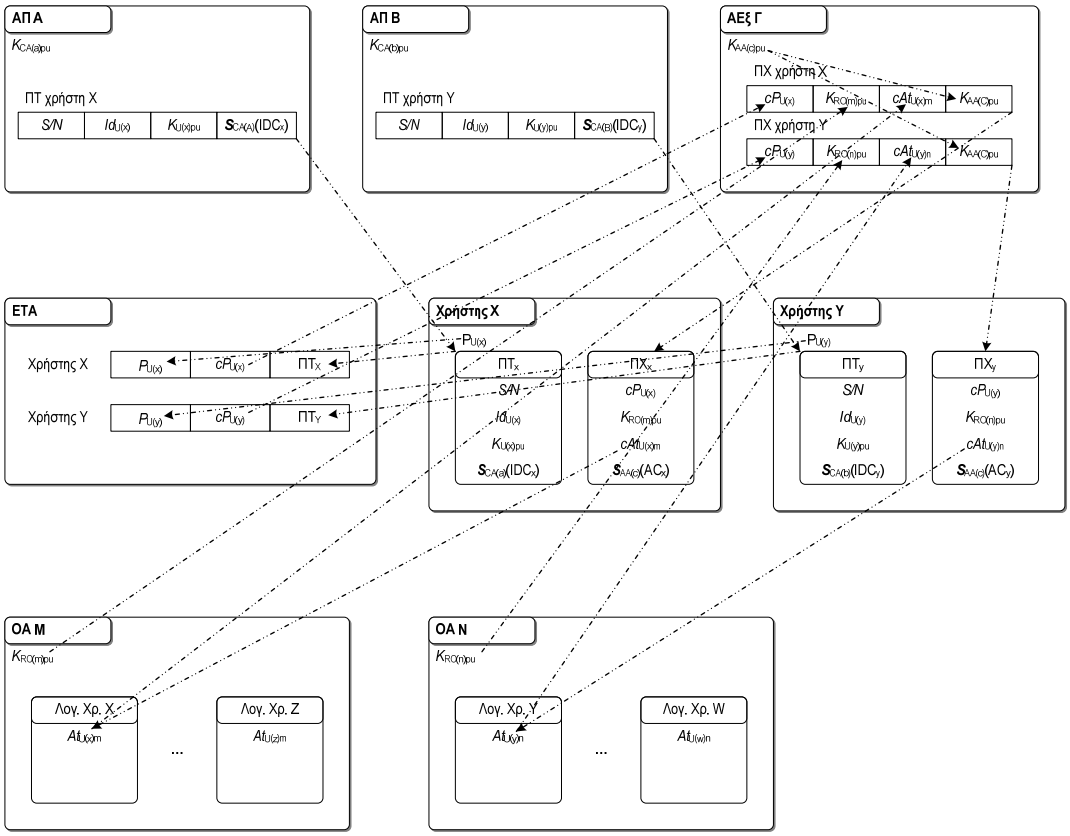
Από την άλλη μεριά, η απόδειξη της κατοχής του ΕΟΑ έχει βασική σημασία, τόσο για τη δημιουργία λογικής σχέσης μεταξύ της συνεδρίας του χρήστη και του λογαριασμού του στο πληροφοριακό σύστημα του ΟΑ, όσο και για την αποφυγή αποκήρυξης ευθύνης συναλλαγών (μπορεί να χρησιμοποιηθεί και εναλλακτικά των απλών διαπιστευτηρίων). Τυπικά, η προμήθεια του ΕΟΑ γίνεται από ΕΓ του ΟΑ, μπορεί όμως να εκδοθεί και επιγραμμικά. Παραδείγματα ΕΟΑ είναι ο ΑΦΜ, ΑΜΚΑ, αριθμός δημοτολογίου, κωδικός πελάτη κλπ. Ο ΕΟΑ είναι ειδικός για κάθε ΟΑ και πιθανώς για μία συγκεκριμένη εφαρμογή του. Ως αποτέλεσμα ένας χρήστης διαθέτει τυπικά πολλούς ΕΟΑ, τουλάχιστον έναν για κάθε ΟΑ. Η βασική χρησιμότητα του προτεινόμενου μοντέλου

ΥΔΚ είναι η ισχυρή και μη αποκηρύξιμη τεχνική σύνδεση των ΕΟΑ με την ψηφιακή αναπαράσταση της ταυτότητας του χρήστη (ΠΤ), ενώ διασφαλίζονται οι παραπάνω απαιτήσεις. Ένα επιπλέον θετικό είναι ότι τα ΕΟΑ συνδέονται αυτόματα με το ΠΤ και δεν χρειάζονται διαχείριση από τον χρήστη.

Συνεχίζοντας τη διαδικασία που μοντελοποιείται, ο χρήστης πρέπει να αποκτήσει τουλάχιστον ένα ΠΤ από μία ΑΠ χρησιμοποιώντας την τυπική διαδικασία. Με αυτό, δημιουργεί και δηλώνει ένα ψευδώνυμο στην ΕΤΑ, η οποία εμπιστεύεται την ΑΠ. Η ΕΤΑ εκδίδει μια ψευδώνυμη Αίτηση ΠΧ (ΑιΠΧ), η οποία περιέχει το ΕΟΑ του απαιτούμενου ΟΑ (ο οποίος εμπιστεύεται την ΑΕξ). Η ΑιΠΧ προωθείται σε μια ΑΕξ (που εμπιστεύεται την ΕΤΑ) και αυτή εκδίδει το ψευδώνυμο ΠΧ, το οποίο χρησιμοποιεί ο χρήστης με τον ΟΑ. Με αυτή τη διαδικασία, οι ΟΑ δεν γνωρίζουν (και υπό κανονικές συνθήκες δεν μαθαίνουν ποτέ) την πραγματική πιστοποιημένη ταυτότητα του χρήστη και ακόμα και αν προσπαθήσουν να παρακολουθήσουν τις συναλλαγές του, δεν μπορούν να τις συνδέσουν με την πραγματική ταυτότητά του, χωρίς τη συνδρομή της ΕΤΑ. Μπορούν ωστόσο να ελέγξουν και να επαληθεύσουν τα περιεχόμενα του ΠΧ και του ΕΟΑ που περιέχεται σ' αυτό. Το ίδιο ισχύει και για τις ΑΕξ και ΑΠ. Μόνο με την σύμπραξη και των τεσσάρων (ΟΑ, ΑΕξ, ΕΤΑ και ΑΠ), μπορεί η πραγματική ταυτότητα του χρήστη να αποκαλυφθεί και να συνδεθούν οι συναλλαγές του με αυτήν. Η ΕΤΑ είναι η μόνη πλευρά που καταγράφει τη μοναδική σχέση μεταξύ των ψευδωνύμων (και των συναλλαγών που γίνονται με αυτά) και των πραγματικών ταυτοτήτων των χρηστών. Οι ΑΠ γνωρίζουν τις πραγματικές ταυτότητες (και τα ΠΤ), η ΕΤΑ γνωρίζει τα ψευδώνυμα (και τις συνδέσεις τους με τα ΠΤ), οι ΑΕξ γνωρίζουν τα ΠΧ (και τις συνδέσεις τους με τα ψευδώνυμα) και οι ΟΑ γνωρίζουν τις συναλλαγές (και τις συνδέσεις τους με τα ΠΧ). Αυτός ο κατακερματισμός γνώσης αναχαιτίζει τη σύνδεση μεταξύ της ταυτότητας του χρήστη και των συναλλαγών του και κάνει δύσκολη την παρακολούθηση και διασύνδεσή τους, ενώ κάνει δυνατή (με τη σύμπραξη και των τεσσάρων μερών) την αποφυγή αποκήρυξης ευθύνης της πραγματοποίησής τους.

Οι λογικές σχέσεις μεταξύ των πλευρών που μετέχουν στο προτεινόμενο μοντέλο (ΑΠ, ΕΤΑ, ΑΕξ, ΟΑ, χρηστών) και η μεταφορά των δεδομένων μεταξύ τους (κλειδιά, ψευδώνυμα, χαρακτηριστικά) αναπαρίσταται στο Σχήμα 14. Οι συνδέσεις επικοινωνίας υλοποιούνται με υπηρεσίες web και διασφαλίζουν την εμπιστευτικότητα και ακεραιότητα της επικοινωνίας με χρήση πιστοποιητικών εξυπηρετητών και πρωτόκολλα TLS/SSL. Τα πιστοποιητικά των εξυπηρετητών μπορεί να εκδίδονται από ειδική ΑΠ της ΕΤΑ ή από μία από τις ΑΠ (με τη συγκατάθεση των οργανισμών που συμμετέχουν),

ή μπορεί να είναι ιδιο-υπογεγραμμένα (self-signed), εντός ενός μοντέλου διομότιμης (peer-to-peer) εμπιστοσύνης. Για τους συμβολισμούς, παρακαλώ αναφερθείτε στον Πίνακα 8 του Παραρτήματος Α.



Σχήμα 14. *Συμμετέχοντες, σχέσεις και περιεχόμενα πιστοποιητικών*

Στο μοντέλο υπάρχουν οι ακόλουθες δικλείδες ασφαλείας, οι οποίες προστατεύουν την ταυτότητα του χρήστη και διασφαλίζουν την ανωνυμία των συναλλαγών του:

1) Το ψευδώνυμο του χρήστη περιέχεται στο πεδίο *Holder* του ΠΧ πληρούμενο και κρυπτογραφημένο με το δημόσιο κλειδί της ΕΤΑ. Αυτό εξασφαλίζει ότι το πραγματικό ψευδώνυμο, το οποίο αποτελεί τη σύνδεση με την πραγματική ταυτότητά του στην εσωτερική βάση δεδομένων της ΕΤΑ είναι γνωστό μόνο σ' αυτήν και δεν μπορεί να γίνει συσχέτιση κρυπτο-ψευδωνύμων και ψευδωνύμων.
2) Η ΕΤΑ δεν μαθαίνει ποτέ το ανώνυμο δημόσιο κλειδί του χρήστη. Σαν αποτέλεσμα δεν μπορεί (από μόνη της) να παρακολουθήσει τη χρήση του.
3) Η ΑΕξ δεν γνωρίζει το πραγματικό ψευδώνυμο του χρήστη, μόνο το κρυπτο-ψευδώνυμο και έτσι δεν μπορεί να το συνδέσει με την ταυτότητά του (ακόμα και αν την γνώριζε) χωρίς τη συνδρομή της ΕΤΑ.

4) Τα ΕΟΑ βρίσκονται τυχαίως πληρούμενα και κρυπτογραφημένα (κΕΟΑ) μέσα στο ΠΧ, με το δημόσιο κλειδί του χρήστη. Αυτό σημαίνει ότι χρειάζεται η άδειά του για να απελευθερωθούν και δεν μπορεί να γίνει σύνδεση μεταξύ κΕΟΑ και ΕΟΑ.

4.2.3 Έκδοση πιστοποιητικών

Πιο λεπτομερώς, η έκδοση των πιστοποιητικών ακολουθεί την παρακάτω διαδικασία:

α) Ο χρήστης εγγράφεται σε ένα ΟΑ και προμηθεύεται, είτε μέσω ΕΓ, είτε επιγραμμικά, ένα ειδικό για τον ΟΑ (και πιθανώς για τη συγκεκριμένη εφαρμογή) ΕΟΑ. Ο ΟΑ παρέχει τυπικά στον χρήστη και απλά διαπιστευτήρια (όνομα/κωδικός) για τη σύνδεση με τη συγκεκριμένη εφαρμογή και προαιρετικά με ανώνυμη υλική απόδειξη κατοχής του ΕΟΑ. Αν παρέχεται, αυτή θα υποβληθεί στο ΕΓ της ΑΕξ, παρακάτω στη διαδικασία.

β) Ο χρήστης προμηθεύεται ένα ΠΤ κάνοντας αίτηση στην ΑΠ μέσω μιας ΑΕ, καταθέτοντας τα δικαιολογητικά που αποδεικνύουν την ταυτότητά του σε ένα ΕΓ, όπως σε μια κανονική διαδικασία ταυτοποίησης. Υπογραμμίζεται ότι ο χρήστης δεν μαθαίνει ποτέ το ιδιωτικό του κλειδί K_{Upr}, το οποίο παράγεται και αποθηκεύεται εντός της ΑΔΑΠ.

γ) Χρησιμοποιώντας το ΠΤ, συνδέεται με ασφαλή δίαυλο (SSL/TLS) στην ΕΤΑ (τυπικά με ανακατεύθυνση της ιστοσελίδας του ΟΑ για του οποίου την υπηρεσία ενδιαφέρεται, ή από δημόσια πύλη). Στη διαδικασία σύνδεσης τυπικά διεξάγεται ισχυρή αμοιβαία επαλήθευση ταυτότητας με το πιστοποιητικό του χρήστη και του εξυπηρετητή της ΕΤΑ. Αυτό γίνεται με διαδικασία πρόκλησης, ως ακολούθως (για το συμβολισμό παρακαλώ αναφερθείτε στον Πίνακα 8 του Παραρτήματος Α):

U : $pkc \rightarrow RO$

RO : pkc lookup CRL_{CA}

RO : if (pkc OK and not revoked) then (

RO : $chlng \rightarrow U$

U : $c = E_{\mathrm{Upr}}(chlng)$

U : $c \rightarrow RO$

RO : $m = D_{\mathrm{Upu}}(c)$

RO : if ($chlng = m$) then return *TRUE* else return *FALSE*

)

Αυτή η διαδικασία επαλήθευσης και πρόκλησης δημοσίου κλειδιού πιστοποιητικού (public key certificate verification and challenge) ορίζεται ως συνάρτηση *PKCVC*(*pkc*, *RO*), όπου *pkc* το ΠΤ και RO ο οργανισμός που επαληθεύει την ταυτότητα (σ' αυτή την περίπτωση η ΕΤΑ). Η συνάρτηση επιστρέφει *TRUE* αν η επαλήθευση είναι επιτυχής και *FALSE* αν όχι και θα χρησιμοποιηθεί στους αλγόριθμους παρακάτω.

Μετά την επαλήθευση ταυτότητας η εφαρμογή πλευράς χρήστη (ΕΠΧ) δημιουργεί ένα τυχαίο ψευδώνυμο P_U, σύμφωνα με τις προδιαγραφές της ΕΤΑ, καθώς και ένα ζεύγος ανώνυμων κλειδιών (AK_{Upu}, AK_{Upr}), το οποίο παράγεται και φυλάσσεται εντός της ΑΔΑΠ (και αργότερα συνδέεται με το ΠΧ). Το P_U αποστέλλεται στην ΕΤΑ, η οποία παράγει τη μορφή του cP_U με τυχαία πλήρωση και κρυπτογράφηση με το δημόσιο κλειδί της. Τα P_U, cP_U και ΠΤ αποθηκεύονται ως σύνδεση μεταξύ του ανώνυμου ψευδώνυμου και της ταυτότητας του χρήστη. Σημειώνεται ότι ο χρήστης δεν μαθαίνει ποτέ το ιδιωτικό ανώνυμο κλειδί του AK_{Upr}.

Στη συνέχεια, η ΕΠΕ παρουσιάζει στο χρήστη λίστα των ΟΑ και των αντιστοίχων ΑΕξ που γνωρίζει και με την επιλογή ενός αυτών κατασκευάζει μια ΑιΠΧ, η οποία:

1) στο πεδίο *Holder* περιέχει το κρυπτο-ψευδώνυμο cP_U του χρήστη,
2) στο πεδίο *Attributes* περιέχει το δημόσιο κλειδί K_{ROpu} του ΟΑ που επέλεξε ο χρήστης,
3) είναι ψηφιακά υπογεγραμμένη από την ΕΤΑ και κρυπτογραφημένη με το δημόσιο κλειδί της ΑΕξ, έτσι ώστε να αποφεύγεται επέμβαση και πλαστογράφηση της αίτησης.

Μαζί με την αίτηση παρέχεται ένας σύνδεσμος προς την εφαρμογή της ΑΕξ για την ολοκλήρωση της έκδοσης του ΠΧ. Σημειώνεται ότι η ΕΤΑ δεν μαθαίνει ποτέ το ανώνυμο ζεύγος κλειδιών (AK_{Upu}, AK_{Upr}) του χρήστη.

δ) Μέσω του συνδέσμου που παρείχε η ΕΤΑ, ο χρήστης συνδέεται στην ΑΕξ και αποστέλλει την κρυπτογραφημένη ΑιΠΧ, μαζί με το ανώνυμο δημόσιο κλειδί AK_{Upu} του (το ανώνυμο ιδιωτικό κλειδί AK_{Upr} δεν βγαίνει ποτέ από την ΑΔΑΠ). Η ΕΠΕ της ΑΕξ αποκρυπτογραφεί την αίτηση με το ιδιωτικό της κλειδί και ελέγχει την εγκυρότητα της ψηφιακής υπογραφής της ΕΤΑ. Αν απαιτείται (δείτε το επόμενο βήμα) επιστρέφει στο χρήστη και ένα μοναδικό αδειοδοτικό ασφαλείας (unique security token) ΜΑΑ, κρυπτογραφημένο με το δημόσιο κλειδί της (κΜΑΑ). Σημειώνε-

ται ότι η ΑΕξ δεν μαθαίνει ποτέ το πραγματικό ψευδώνυμο P_U του χρήστη, το οποίο γνωρίζει μόνο η ΕΤΑ, μόνο το cP_U.

ε) Ο χρήστης αποτείνεται στο ΕΓ της ΑΕξ με την υλική απόδειξη της κατοχής του ζητούμενου ΕΟΑ, μαζί με το κΜΑΑ. Το ΕΓ ελέγχει την ορθότητα των αποδεικτικών και επιστρέφει στην ΑΕξ το κΜΑΑ και το ΕΟΑ. Αυτό το βήμα δεν γίνεται αν δεν παρέχεται υλική απόδειξη κατοχής του ΕΟΑ από το ΕΓ του ΟΑ.

στ) Αν χρησιμοποιήθηκε κΜΑΑ, η ΑΕξ το λαμβάνει από το ΕΓ της, το αποκρυπτογραφεί με το ιδιωτικό της κλειδί και αν ταιριάζει με το αρχικό ΜΑΑ που παράχθηκε, προχωρά στο επόμενο βήμα.

ζ) Η ΑΕξ εκδίδει το ΠΧ το οποίο:

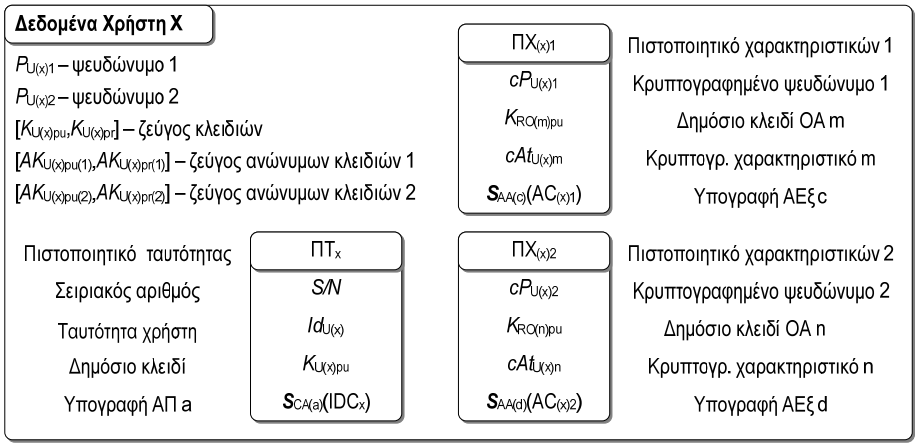
1) στο πεδίο *Holder* περιέχει το (κρυπτογραφημένο) ψευδώνυμο cP_U που περιεχόταν στην ΑιΠΧ,
2) στο πεδίο *Attributes* περιέχει το K_{ROpu} που περιεχόταν στην ΑιΠΧ και το ΕΟΑ πληρούμενο και κρυπτογραφημένο (κΕΟΑ ≡ cAt_U) με το ανώνυμο δημόσιο κλειδί AK_{Upu} του χρήστη.

Τέλος, η ΑΕξ αποθηκεύει τη σχέση σειριακού αριθμού ΠΧ – ανώνυμου δημόσιου κλειδιού χρήστη – κρυπτο-ψευδωνύμου και ειδοποιεί το χρήστη για την έκδοση του ΠΧ, μαζί με σύνδεσμο για την παραλαβή του.

η) Μέσω του συνδέσμου, ο χρήστης συνδέεται στην ΕΠΕ της ΑΕξ, η οποία στέλνει το εκδοθέν ΠΧ και το σχετικό AK_{Upu} που χρησιμοποιήθηκε κατά την ΑιΠΧ. Η ΕΠΧ τα παραλαμβάνει και εγκαθιστά το ΠΧ, μαζί με μια σύνδεση προς το σχετικό ανώνυμο ζεύγος κλειδιών (AK_{Upu}, AK_{Upr}) στην ΑΔΑΠ.

θ) Η διαδικασία επαναλαμβάνεται από το βήμα (β) για κάθε ΠΧ/ΕΟΑ/ΟΑ που επιθυμεί ο χρήστης, έτσι ώστε να διαθέτει διαφορετικό ψευδώνυμο και ζεύγος ανώνυμων κλειδιών για κάθε ΠΧ και ΟΑ. Αυτό από τη μια δυσκολεύει τη συσχέτιση και παρακολούθηση των συναλλαγών του και παρεμποδίζει πιθανή κακόβουλη συνεργασία ΑΕξ/ΟΑ και από την άλλη εξασφαλίζει ότι με τη λήξη ενός ψευδώνυμου (εφόσον λήγει, βλ. παρακάτω) δεν θα πρέπει να επανεκδοθούν όλα τα ΠΧ, παρά μόνο αυτό που αφορά το ψευδώνυμο που λήγει.

Στο Σχήμα 15 αυτό παρουσιάζονται τα δεδομένα που φυλάσσονται στην ΑΔΑΠ του χρήστη και τα περιεχόμενα των πιστοποιητικών.



Σχήμα 15. *Δεδομένα χρήστη και περιεχόμενα πιστοποιητικών*

Η διαδικασία (περιλαμβάνοντας και την έκδοση του ΠΤ) περιγράφεται στο ακόλουθο πρωτόκολλο (για το συμβολισμό παρακαλώ αναφερθείτε στον Πίνακα 8 του Παραρτήματος Α):

U : $(UN_U, PW_U) \rightarrow RO$

RO : $At_U \rightarrow U$

U : $(K_{Upu}, K_{Upr}) = NAK()$

U : $STORE((K_{Upu}, K_{Upr}))$

U : $z = NSK()$

U : $[z, PKCR(Id_U, K_{Upu})] \rightarrow RA$

RA : $y = OTP() \rightarrow U$

U : $Id_U \rightarrow CO_{RA}$

CO_{RA} : $Id_U \rightarrow RA$

RA : $[y, z, PKCR(Id_U, K_{Upu})] \rightarrow CA$

CA : $cb = nPKCb(PKCR(Id_U, K_{Upu}))$

CA : $pkc = cb + E_{CApr}(H(cb))$

CA : $c = E_z(pkc)$

U : $y \rightarrow CA$

CA : $c \rightarrow U$

U : $pkc' = D_z(c)$

U : $IC(pkc', K_{Upu})$

U : $pkc' \rightarrow TTP$

if (not $PKCVC(pkc', TTP)$) then abort

U : $(AK_{Upu}, AK_{Upr}) = NAK()$

U : $STORE((AK_{Upu}, AK_{Upr}))$

U : $P_U = NRID() \rightarrow TTP$

TTP : $pad = OTP()$

TTP : $cP_U = E_{TTPpu}(P_U + pad)$

TTP : $STORE(P_U, cP_U, pkc')$

TTP : $acr = ACR(cP_U, K_{ROpu})$

TTP : $e = E_{AApu}(S_{TTP}(acr)) \rightarrow U$

U : $w = NSK()$

U : $(e, w, AK_{Upu}) \rightarrow AA$

AA : $acr' = D_{AApr}(e)$

AA : if not $V^2_{TTP}(acr')$ then abort

AA : $UST = OTP()$

AA : $cUST = E_{AApu}(UST) \rightarrow U$

U : $(cUST, At_U) \rightarrow CO_{AA}$

CO_{AA} : $(cUST, At_U) \rightarrow AA$

AA : if $(UST \mathrel{!}= D_{AApr}(cUST))$ then abort

AA : $ac = nACb(acr', At_U)$

AA : $g = E_w(ac)$

AA : $STORE(ESN(ac), AK_{Upu}, cP_U)$

AA : $(g, AK_{Upu}) \rightarrow U$

U : $ac' = D_w(g)$

U : $IC(ac', AK_{Upu})$

Τα σημεία της διαδικασίας που διαφέρουν από μια συμβατική έκδοση ΠΤ έχουν σκιαστεί και αφορούν τη δημιουργία του ψευδωνύμου και την έκδοση της ΑιΠΧ και του ΠΧ. Η διαδικασία προστατεύεται από συμμετρική (μεταφορά ΠΤ και ΠΧ) και ασύμμετρη (μεταφορά ΑιΠΧ, ψευδωνύμου και ΜΑΑ) κρυπτογράφηση, έτσι ώστε να αποκρούονται προσπάθειες παραχάραξης αιτήσεων πιστοποιητικών, ψευδωνύμων και ΜΑΑ από τους χρήστες και τρίτους και να διασφαλίζεται η εμπιστευτικότητα των πιστοποιητικών.

4.2.4 Χρήση πιστοποιητικών

Η χρήση των πιστοποιητικών γίνεται ως ακολούθως:

α) Προκειμένου να συναλλαχθεί με έναν ΟΑ, ο χρήστης τυπικά παρουσιάζει τα απλά διαπιστευτήρια (όνομα/κωδικός) που του έχουν δοθεί (εφόσον απαιτείται) στην εφαρμογή. Λαμβάνεται ως δεδομένο ότι τα διαπιστευτήρια αυτά δεν αποτελούν ισχυρή απόδειξη της ταυτότητάς του ή κατοχής του ΕΟΑ και δεν είναι υποχρεωτικά, βοηθούν όμως στη δημιουργία μιας συνεδρίας (session) με την ΕΠΕ του ΟΑ. Η επαλήθευση ταυτότητας δεν πρέπει να γίνεται με το ΠΤ, καθώς αυτό θα ακύρωνε τη ζητούμενη ανωνυμία και θα καθιστούσε τη συσχέτιση και παρακολούθηση των συναλλαγών του χρήστη από τον ΟΑ (και τρίτους) εύκολη, με τον σειριακό αριθμό του ΠΧ. Ο χρήστης χρειάζεται να αποδείξει κατοχή μόνο του ζητούμενου ΕΟΑ.

β) Η ΕΠΧ επιλέγει από την ΑΔΑΠ το ΠΧ που αντιστοιχεί σε αυτόν τον ΟΑ, βάση του K_{ROpu} που περιέχει και το αποστέλλει στην ΕΠΕ του ΟΑ.

γ) Η ΕΠΕ διενεργεί έλεγχο εγκυρότητας του ΠΧ (δημόσιο κλειδί, ψηφιακή υπογραφή και ΚΑΠ της ΑΕξ) και εφόσον είναι αποδεκτό η διαδικασία προχωράει.

δ) Η ΕΠΧ αποκρυπτογραφεί το κΕΟΑ (cAt_{U}) με το ανώνυμο ιδιωτικό κλειδί του χρήστη AK_{Upu} (με ερώτηση του pin και άρα της συναίνεσης του) και το αποστέλλει στην ΕΠΕ (υπενθυμίζεται ότι το κΕΟΑ μπορεί να αποκρυπτογραφηθεί μόνο με το ανώνυμο ιδιωτικό κλειδί του χρήστη). Αυτό αποδεικνύει την κατοχή του ανώνυμου ιδιωτικού κλειδιού και αποτρέπει την πλαστογράφηση (μέσω της ψηφιακής υπογραφής της ΑΕξ) και το δανεισμό των πιστοποιητικών (ο ίδιος ο χρήστης δεν γνωρίζει το ιδιωτικό του κλειδί, το οποίο δεν βγαίνει από την ΑΔΑΠ, μόνο το pin). Το ΠΧ καταγράφεται στον λογαριασμό του χρήστη και μετέπειτα συναλλαγές αυτής της συνεδρίας αφορούν το συγκεκριμένο λογαριασμό. Σαν αποτέλεσμα, η συνεδρία έχει συνδεθεί ισχυρά με το λογαριασμό του χρήστη και η εξουσιοδότησή του έχει επιτευχθεί.

ε) Σε εφαρμογές ψηφιακής υπογραφής συναλλαγής, στο βήμα (δ) θα πρέπει να αποσταλεί από την ΕΠΧ και το ανώνυμο δημόσιο κλειδί του χρήστη AK_{Upu} και να αποθηκευτεί στο λογαριασμό του. Από κει και πέρα η ΕΠΧ υπογράφει με το ανώνυμο ιδιωτικό κλειδί του χρήστη AK_{Upr} που περιέχεται στην ΑΔΑΠ (μετά από ερώτηση του pin) και η ΕΠΕ επαληθεύει με το ανώνυμο δημόσιο κλειδί του χρήστη AK_{Upu} που υπάρχει στο λογαριασμό του από το προηγούμενο βήμα.

Η διαδικασία περιγράφεται στο ακόλουθο πρωτόκολλο (για το συμβολισμό παρακαλώ αναφερθείτε στον Πίνακα 8 του Παραρτήματος Α).

$$U: \ (UN_{\mathrm{U}}, PW_{\mathrm{U}}) \rightarrow RO$$

U : $AC \rightarrow RO$

RO : if not valid(AC) then abort

U : $OSID = D_{\mathrm{Upr}}(cAt_{\underline{U}}) \rightarrow RO$

Εφόσον ο ΟΑ διαπιστώσει κακή συμπεριφορά από το χρήστη, μπορεί να αποταθεί στην ΑΕξ προκειμένου καταρχήν να ανακληθεί το αντίστοιχο ΠΧ. Αν απαιτείται αποκάλυψη της πραγματικής του ταυτότητας, μπορεί να συμπράξει με την ΑΕξ και την ΕΤΑ για να αποκρυπτογραφηθεί (με το ιδιωτικό της κλειδί) το πεδίο *Holder* του ΠΧ που έχει χρησιμοποιηθεί κακόβουλα, να αποκαλυφθεί το πραγματικό ψευδώνυμο P_{U} του χρήστη και μέσω της σύνδεσής του με το ΠΤ να προσδιοριστεί η ταυτότητά του.

Μόνο με ταυτόχρονη γνώση του σειριακού αριθμού του ΠΧ, του ανώνυμου δημόσιου κλειδιού του χρήστη, του πραγματικού (ακρυπτογράφητου) ψευδωνύμου του και του ΠΤ του μπορεί να γίνει σύνδεση των συναλλαγών του χρήστη με την πραγματική ταυτότητά του και αυτό μπορεί να γίνει μόνο με σύμπραξη ΕΤΑ, ΑΕξ και ΟΑ.

4.2.5 Ανάκληση πιστοποιητικών

Όσον αφορά τα ΠΤ, καθώς πρόκειται για τυπικά X.509 πιστοποιητικά, η διαδικασία ανάκλησής τους δεν διαφέρει από τις συμβατικές ΥΔΚ. Όσον αφορά τα ΠΧ, η ανάκληση ενός ΠΤ δεν απαιτεί υποχρεωτικά ανάκληση των ΠΧ, καθώς το ΠΤ δεν χρησιμοποιείται για τις συναλλαγές. Διακρίνουμε τις ακόλουθες περιπτώσεις:

α) Η ανάκληση του ΠΤ ζητείται από τον χρήστη.

Σε αυτή την περίπτωση, η ΑΠ πρέπει να παρέχει τη δυνατότητα ανάκλησης των ΠΧ που έχουν εκδοθεί βάσει του ΠΤ. Γι' αυτό το σκοπό, η ΑΠ πρέπει να τοποθετήσει το ΠΤ σε ειδικό ΚΑΠ που παρακολουθείται από την ΕΤΑ. Αυτό έχει σαν αποτέλεσμα την ανάκληση των σχετικών ψευδωνύμων και τοποθέτηση των κρυπτοψευδωνύμων (cP_{U}) σε ειδικό ΚΑΠ της ΕΤΑ. Οι ΑΕξ και οι ΟΑ θα πρέπει να τον παρακολουθούν και να ανακαλέσουν / σταματήσουν να δέχονται τα σχετικά ΠΧ.

β) Η ανάκληση του ΠΤ γίνεται από την εκδίδουσα ΑΠ.

Σε αυτή την περίπτωση, τα σχετικά ψευδώνυμα και ΠΧ δεν χρειάζονται ανάκληση, καθώς ανάκληση της ταυτότητας δεν συνδέεται απαραίτητα με ανάκληση των χαρακτηριστικών. Διαφορετικά αυτό θα πρέπει να αναφέρεται ρητώς στις ΔΠΠ των ΑΕξ, ΕΤΑ και ΟΑ και να γίνουν οι ενέργειες του βήματος (α).

γ) Η ανάκληση του ΠΧ ζητείται από τον χρήστη. Διακρίνουμε δύο υπο-περιπτώσεις:

i) Ανάκληση όλων των ΠΧ που εκδόθηκαν βάσει ενός ΠΤ.

Σε αυτή την περίπτωση ο ιδιοκτήτης συνδέεται στην ΕΠΕ της ΕΤΑ και, μετά από διαδικασία επαλήθευσης ταυτότητας πρόκλησης-απόκρισης με το ΠΤ του, μπορεί να ανακαλέσει όλα τα ψευδώνυμα που έχουν εκδοθεί με το ΠΤ. Αυτό προκαλεί τοποθέτηση των σχετικών κρυπτο-ψευδωνύμων στον ΚΑΠ της ΕΤΑ, η οποίος παρακολουθείται από τις ΑΕξ και τους ΟΑ. Αυτό με τη σειρά προκαλεί ανάκληση όλων των σχετικών ΠΧ και την απόρριψή τους από τους ΟΑ.

ii) Ανάκληση ενός ΠΧ.

Σε αυτή την περίπτωση θα πρέπει να έχει διατεθεί στο χρήστη εφαρμογή διαχείρισης ΠΧ. Αυτή παρέχεται από την ΕΤΑ και θα πρέπει να προτείνεται για εγκατάσταση κατά την αρχική έκδοση ψευδωνύμου. Με αυτή την εφαρμογή ο χρήστης μπορεί να κάνει ανασκόπηση των ΠΧ που υπάρχουν στην ΑΔΑΠ του, μαζί με τους σχετικούς ΟΑ και να έχει την δυνατότητα να ανακαλέσει ένα ή περισσότερα. Αυτό θα προκαλέσει σύνδεση με την αντίστοιχη ΑΕξ και θα κάνει δυνατή την ανάκληση του συγκεκριμένου ΠΧ.

δ) Η ανάκληση ΠΧ ζητείται από τον ΟΑ.

Καθώς τα ΠΧ και τα ΠΤ βρίσκονται στην κατοχή του χρήστη, σε περίπτωση που ένας ΟΑ απαιτεί την αλλαγή ή ανάκληση ΕΟΑ που έχει εκδοθεί από αυτόν, δεν μπορεί να αιτηθεί την ανάκληση είτε του σχετικού ΠΧ, είτε του ΠΤ. Όμως, επειδή αποθηκεύει τα ΠΧ, μπορεί απλά να σταματήσει να δέχεται το ΠΧ που αντιστοιχεί στο υπό αλλαγή/ανάκληση ΕΟΑ και έτσι να υποχρεώσει τον χρήστη στην προμήθεια νέου με τον νέο ΕΟΑ.

4.2.6 Ανανέωση πιστοποιητικών

Η ανανέωση των ΠΤ γίνεται όπως και σε συμβατικές ΥΔΚ. Για την ανανέωση των ΠΧ, διακρίνουμε δύο περιπτώσεις.

α) Τα ψευδώνυμα λήγουν και έχουν μικρότερη διάρκεια ισχύος από τα ΠΧ.

Αν τα ψευδώνυμα λήγουν (το οποίο είναι προφανώς πιο ασφαλές), η λήξη ενός κάνει απαραίτητη την ανάκληση του αντίστοιχου ΠΧ και την έκδοση νέου που συνδέεται με τον νέο ψευδώνυμο. Η ΕΤΑ πρέπει να παρακολουθεί την εγκυρότητά τους και με την προσεχή λήξη ενός, να ειδοποιεί το χρήστη και να τον οδηγεί στην παραγωγή νέου ψευδώνυμου, ανώνυμου ζεύγους κλειδιών και ΠΧ, με την ίδια διαδικασία όπως στην αρχική έκδοση. Οι ΑΕξ και ΟΑ απλώς παρατηρούν (και εκδίδουν και παρακολουθούν) τη χρήση νέων έγκυρων ΠΧ. Για προστασία από συνεχιζόμενη χρήση ΠΧ των οποίων τα ψευδώνυμα έχουν λήξει, η ΕΤΑ πρέπει να δημοσιεύει κα-

τάλογο cP_U που έχουν λήξει και οι ΑΕξ και ΟΑ να τον παρακολουθούν και να ανακαλούν/σταματούν να δέχονται τα σχετικά ΠΧ.

β) Τα ψευδώνυμα δεν λήγουν, ή έχουν μεγαλύτερη διάρκεια ισχύος από τα ΠΧ.
Σε αυτή την περίπτωση ένα ΠΧ μπορεί να λήξει πριν το σχετικό ψευδώνυμο. Τότε ο χρήστης πρέπει να υποχρεώνεται και να οδηγείται από τον ΟΑ για την έκδοση νέου ΠΧ (με ένα σύνδεσμο στην ΕΤΑ), έτσι ώστε η διαδικασία να ξεκινήσει από το βήμα (β) έκδοσης ΠΧ, αλλά χωρίς την δημιουργία νέου ψευδωνύμου και ανώνυμου ζεύγους κλειδιών. Για απλότητα και ευκολία χρήσης προτείνεται τα ψευδώνυμα να έχουν την ίδια διάρκεια εγκυρότητας με τα ΠΧ.

4.2.7 Ανάκτηση κλειδιών

Λόγω της ανώνυμης φύσης στοιχείων του μοντέλου και τον κατακερματισμό γνώσης των συμμετεχόντων, η μεσεγγύηση κλειδιών (key escrow) δεν είναι δυνατή. Ο χρήστης δεν γνωρίζει τα ιδιωτικά του κλειδιά και δεν υπάρχει απαίτηση να τα αποθηκεύουν οι ΑΠ. Η ΕΤΑ, δοθέντος του ΠΤ θα μπορούσε να παρέχει τα ψευδώνυμα, όμως δεν γνωρίζει (και δεν καταγράφει) το ανώνυμο ζεύγος κλειδιών (AK_{Upu}, AK_{Upr}) που αντιστοιχεί σε ένα ψευδώνυμο. Τέλος, η ΑΕξ, δεδομένου του κρυπτο-ψευδώνυμου, θα μπορούσε να παρέχει το ΠΧ, αλλά το cP_U δεν είναι ιδιωτική γνώση και ο χρήστης δεν γνωρίζει το ανώνυμο ιδιωτικό του κλειδί. Σαν αποτέλεσμα, σε περίπτωση απώλειας ΑΔΑΠ (ή του pin και puk της) τα αντίστοιχα ΠΤ, ψευδώνυμα, κλειδιά και ΠΧ πρέπει να ανακληθούν και να επανεκδοθούν με την κανονική διαδικασία.

4.2.8 Απειλές για την ασφάλεια και αντίμετρα

Οι πιθανές απειλές για την ασφάλεια του μοντέλου και οι τρόποι που αυτές μετριάζονται είναι οι ακόλουθες:

α) Απειλή αποκάλυψης ή/και πλαστογράφησης με επίθεση στους αλγόριθμους κρυπτογράφησης.
Προτείνεται χρήση των αλγόριθμων συμμετρικής κρυπτογράφησης AES (NIST, 2001), Serpent (http://www.cl.cam.ac.uk/~rja14/serpent.html) ή Twofish (Schneier et al., 1998), με μήκος κλειδιού τουλάχιστον 256 bits. Αυτοί θεωρούνται αυτή τη στιγμή επαρκώς ασφαλείς για την προστασία της υποδομής (CNSS, 2003). Για κρυπτογράφηση δημοσίου κλειδιού προτείνεται ο RSAES-PKCS1-v1_5 (http://www.rsa.com/rsalabs/node.asp?id=2125) και για υπογραφή είτε ο RSASSA-

PKCS1-v1_5, είτε ο DSA (http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf). Αυτοί θεωρούνται επίσης επαρκώς ασφαλείς.

β) Απειλή πλαστογράφησης με επίθεση στους αλγόριθμους κατακερματισμού.
Προτείνεται η χρήση των αλγορίθμων κατακερματισμού RIPEMD-160, SHA-2 (SHA-256 to SHA-512) ή Whirlpool, οι οποίοι θεωρούνται αυτή τη στιγμή απαραβίαστοι (ISO/IEC, 2004).

γ) Απειλή κοινής χρήσης διαπιστευτηρίων/πιστοποιητικών/χαρακτηριστικών.
Οι ιδιοκτήτες των ΠΤ και ΠΧ δεν μαθαίνουν ποτέ τα ιδιωτικά τους κλειδιά, πάνω στα οποία βασίζεται η ασφάλεια του μοντέλου. Αυτά παράγονται και φυλάσσονται εντός της ΑΔΑΠ, το οποίο καθιστά την κοινή χρήση του αδύνατη, όσο δεν παραβιάζεται ο μηχανισμός προστασίας της ΑΔΑΠ. Επίσης, κοινή χρήση των ΕΟΑ είναι άχρηστη, καθώς οι ΟΑ ελέγχουν την εγκυρότητα των ΠΧ και η μεταφορά των ΕΟΑ βασίζεται στη γνώση των ιδιωτικών κλειδιών. Οι ΑΔΑΠ θα πρέπει να είναι τουλάχιστον επιπέδου FIPS 140-2 level 2, το οποίο θεωρείται απαραβίαστο αυτή τη στιγμή (http://www.niap-ccevs.org/pp/pp_pkikmi_tkn_mr_v3.0.pdf).

δ) Απειλή ιδιοποίησης ΕΟΑ.
Η ασφάλεια των ΕΟΑ βασίζεται στις πολιτικές ασφαλείας των ΟΑ που τα εκδίδουν. Αν κάποιος κακόβουλος μπορεί να αποκτήσει αποδεικτικά ιδιοκτησίας ενός ΕΟΑ που να είναι αποδεκτά από το ΕΓ ενός ΟΑ, τότε θα μπορούσε θεωρητικά να συνδέσει ένα άλλο ΠΤ με το ΕΟΑ μέσω δικού του ΠΧ (ένας παραχαράκτης δεν μπορεί να διαμορφώσει ένα ΠΧ χωρίς να ακολουθήσει τη διαδικασία έκδοσης ΠΧ γιατί δεν διαθέτει το ιδιωτικό κλειδί της ΑΕξ και δεν μπορεί να συνδέσει τη συνεδρία του με το ΕΟΑ χωρίς ένα ΠΧ). Ωστόσο σε αυτή την περίπτωση, ο ΟΑ μπορεί εύκολα να ανιχνεύσει διπλότυπη σύνδεση ΠΧ, να μπλοκάρει τη χρήση «πειρατικών» ΕΟΑ και να αιτηθεί στην ΑΕξ και την ΕΤΑ αποκάλυψη ταυτότητας.

4.2.9 Αποτελέσματα

Το πρόβλημα απορρήτου που παρουσιάστηκε είναι δύσκολο να αντιμετωπιστεί διότι περιλαμβάνει αντικρουόμενες απαιτήσεις. Από τη μια μεριά απαιτείται η χρήση συμβατικών ΠΤ. Από την άλλη πρέπει να διασφαλιστεί η προστασία των προσωπικών δεδομένων και η ελευθερία βούλησης του ατόμου.

Όπως φαίνεται στη βιβλιογραφία, η κύρια ερευνητική προσέγγιση του θέματος τα τελευταία χρόνια έχει κατευθυνθεί μακριά από εμπορικά και ανοικτού κώδικα συστήματα ΥΔΚ (στα οποία η τεχνολογία έχει σε μεγάλο βαθμό παγιωθεί) και έχει επικε-

ντρωθεί στις ανώνυμες συναλλαγές και διαπιστευτήρια, με νέα κρυπτογραφικά αρχέγονα και διαδικασίες, που εφαρμόζονται κυρίως σε κινητά και ασύρματα δίκτυα. Ωστόσο, αυτά απαιτούν σημαντική προσπάθεια ανάπτυξης, ξεφεύγουν από εθνικά και διεθνή πρότυπα και εμπορικό λογισμικό και για το λόγο αυτό δεν έχουν υλοποιηθεί σε καμία μεγάλου μεγέθους ιδιωτική ή εθνική ΥΔΚ. Όταν χρειάστηκε η παρουσία χαρακτηριστικών για ταυτοπροσωπία, εξουσιοδότηση ή αποφυγή αποκήρυξης ευθύνης, ακολουθήθηκε η απλή μέθοδος του να συμπεριληφθούν εντός των ΠΤ, χωρίς προσοχή στην προστασία προσωπικών δεδομένων.

Η προσέγγιση που ακολουθούμε σ' αυτή την πρόταση προσπαθεί να κρατήσει το έργο ανάπτυξης νέου λογισμικού στο ελάχιστο (τόσο για τις ΑΠ, ΕΤΑ και ΑΕξ όσο και για τους ΟΑ), βρισκόμενη απολύτως εντός της σύστασης Χ.509 και χρησιμοποιώντας εμπορικούς αλγόριθμους συμμετρικής και ασύμμετρης κρυπτογράφησης και κατακερματισμού. Αυτά, ενώ έχει δομή κατάλληλη για ανάπτυξη σε μεγάλο μέγεθος, χωρίς να κάνει μεγάλες παραχωρήσεις στην ανωνυμία και στην κρυπτογραφική προστασία της ταυτότητας των χρηστών.

Τα ως αποτέλεσμα κύρια σημεία του μοντέλου έχουν ως ακολούθως. Πρώτον, μόνο ένα ΠΤ χρειάζεται σε κάθε χρήστη, ενώ η ύπαρξη πολλών ΠΤ (και ΑΠ) επιτρέπεται. Ένα ΠΤ περιέχει μόνο την ταυτότητα του χρήστη και μπορεί να χρησιμοποιηθεί σε εφαρμογές επαλήθευσης ταυτότητας και ψηφιακής υπογραφής, όπως επιθυμεί ο ιδιοκτήτης του και επιτρέπεται από την ΠΠ της κατατομής του. Δεύτερον, οι ΟΑ δεν μπορούν να διακρίνουν την ταυτότητα του χρήστη και η απελευθέρωση χαρακτηριστικών είναι υπό τον απόλυτο έλεγχό του. Κατά τη σύνδεση με έναν ΟΑ, ο χρήστης χρησιμοποιεί μόνο το ΠΧ, το οποίο πιστοποιεί την κατοχή του χαρακτηριστικού που περιέχει, αλλά δεν περιλαμβάνει σύνδεση με το ΠΤ, μόνο ένα ψευδώνυμο που έχει παραχθεί από τον ίδιο το χρήστη. Οι ΟΑ μπορούν ωστόσο να επαληθεύσουν την κατοχή του ΕΟΑ και την εγκυρότητα/ακεραιότητα του ΠΧ. Τρίτον, το μοντέλο ικανοποιεί τις απαιτήσεις που τέθηκαν από τις παραμέτρους του προβλήματος, ως εξής:

α) Το μοντέλο μπορεί να αναπτυχθεί σε μεγάλης κλίμακας ΥΔΚ. Προβλέπει τη συμμετοχή πολλών ΑΠ, ΑΕξ και ΟΑ και χρήση ΑΕ και ΕΓ, αν απαιτείται. Μόνο η ΕΤΑ είναι μοναδιαία οντότητα, αλλά αυτό δεν αποτελεί πρόβλημα, διότι ο ρόλος της είναι καθαρά τεχνικός και δεν ενέχει προσωπική διεπαφή με τους χρήστες. Επίσης οι ΟΑ δεν εμπιστεύονται απλώς τη ρίζα.

β) Το μοντέλο χρησιμοποιεί εμπορικούς συμμετρικούς και ασύμμετρους (δημοσίου κλειδιού) αλγόριθμους κρυπτογράφησης και τυπικά ΠΤ και ΠΧ, ενώ προάγει τη συμμετοχή πολλών ΑΠ και ΑΕξ. Τα ΠΤ δεν είναι ανώνυμα και δεν εκδίδονται από τους ΟΑ που υλοποιούν τις εφαρμογές.

γ) Τα χαρακτηριστικά (προσωπικά δεδομένα) των χρηστών (ΕΟΑ) προστατεύονται, καθώς υπάρχουν εντός των ΠΧ κρυπτογραφημένα (κΕΟΑ). Η απελευθέρωσή τους, για την ολοκλήρωση μιας συναλλαγής ή μια διαδικασία εξουσιοδότησης/επαλήθευσης ταυτότητας, απαιτεί την ρητή συναίνεση του ιδιοκτήτη (ο οποίος πρέπει να δώσει το pin του).

δ) Καθώς διαφορετικό ΠΧ απαιτείται για κάθε ΕΟΑ που αντιστοιχεί σε έναν ΟΑ, διασφαλίζεται ότι μη απαραίτητα για την ολοκλήρωση της συναλλαγής δεδομένα δεν παρέχονται στους ΟΑ ή σε τρίτους.

ε) Οι μηχανισμοί που παρέχονται από το μοντέλο (κρυπτογραφημένα, τυχαία πληρούμενα, απελευθερώσιμα από το χρήστη και διαφορετικά για κάθε ΟΑ ΕΟΑ), καθιστούν την καθιέρωση καθολικού αναγνωριστικού πολύ δύσκολη και παρέχουν διασφάλιση ότι δεν δίδονται κίνητρα ή ευκαιρίες για την υιοθέτηση από έναν οργανισμό χαρακτηριστικού ταυτοποίησης που αντιστοιχεί σε άλλον.

στ) Το μοντέλο παρέχει ισχυρό και ασφαλή μηχανισμό για την αντιστοίχιση της ταυτότητας σε ένα ή περισσότερα ΕΟΑ, ενώ εμποδίζει την *de-facto* καθιέρωση ΚΑΤ.

Ενώ ικανοποιεί τους στόχους που τέθηκαν, θα πρέπει να αναφερθούν τα ακόλουθα για το μοντέλο. Πρώτον, ο χρήστης πρέπει να διαθέτει πολλαπλά ΠΧ, ένα για κάθε ΟΑ με τον οποίο συναλλάσσεται και μπορεί να πρέπει να αιτηθεί στην ΕΤΑ και στα ΕΓ των ΑΕξ πολλαπλές φορές για την έκδοσή τους. Δεύτερον, η προστασία της ταυτότητας του χρήστη τελικά βασίζεται στην πολιτική ασφαλείας (και την τήρησή της) πολλαπλών οργανισμών, δηλαδή των ΑΠ, ΕΤΑ, ΑΕξ και ΟΑ. Το μοντέλο κάνει δύσκολη την υπέρβαση της προστασίας, τη συσχέτιση των συναλλαγών και την παρακολούθηση των χρηστών, αλλά με συνεργασία μεταξύ των οργανισμών είναι δυνατή. Η πλήρης απαγόρευση αυτής της δυνατότητας θα έκανε τη χρήση σχημάτων πλήρους ανωνυμίας υποχρεωτική και θα δυσκόλευε πολύ την αποφυγή αποκήρυξης ευθύνης των συναλλαγών. Τρίτον, το μοντέλο δεν παρέχει στον χρήστη τη δυνατότητα να αποσύρει τα προσωπικά του στοιχεία από την ΕΤΑ. Θεωρητικά, η ΕΤΑ θα μπορούσε να παρέχει ένα περιβάλλον διαχείρισης από τον χρήστη, αλλά αυτό θα έπρεπε να είναι μόνο για διάβασμα, διαφο-

ρετικά θα καταστρατηγούνταν οι πολιτικές ασφαλείας των ΑΠ. Ακόμα και τότε, δεν θα προστατευόταν ο χρήστης από κακόβουλες πρακτικές της ΕΤΑ. Τέταρτον, η κοινή χρήση ΑΔΑΠ και pin μεταξύ των χρηστών θα πρέπει να τονίζεται ως παράνομη από τις πολιτικές ασφάλειας των οργανισμών που μετέχουν, τις οποίες οι χρήστες θα πρέπει να δεσμεύονται ότι ακολουθούν. Τέλος, υπάρχει αυξημένη πολυπλοκότητα των ΕΠΕ και ΕΠΧ της ΕΤΑ, ΑΕξ και ΟΑ, καθώς και αυξημένες απαιτήσεις αποθήκευσης στις Α-ΔΑΠ για τα ΠΧ, ψευδώνυμα και ζεύγη ανωνύμων κλειδιών.

4.2.10 Εφαρμογή της προτεινόμενης μεθοδολογίας ΑΔ στην πρωτότυπη ΥΔΚ

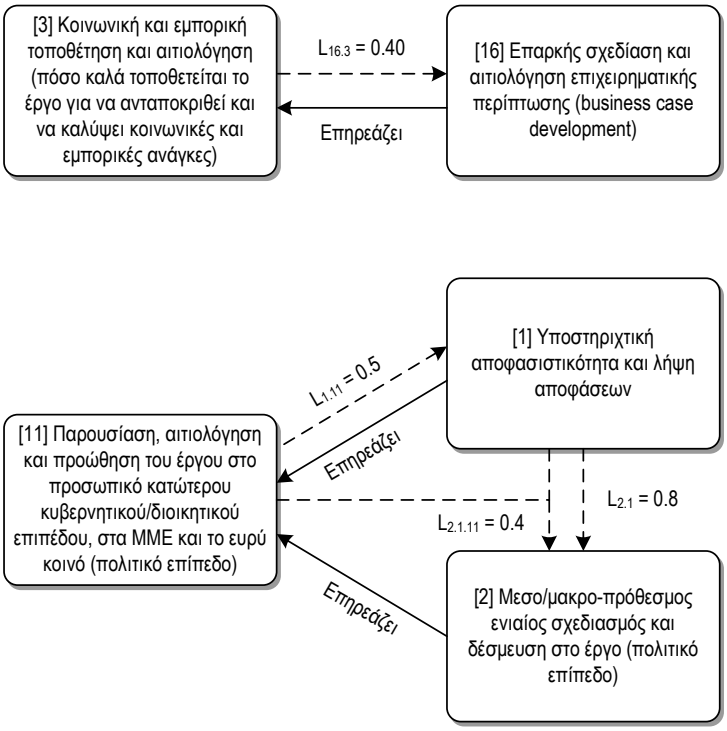
Σε αυτό το σημείο θα γίνει δοκιμή της προτεινόμενης μεθοδολογίας ΑΔ στην πρωτότυπη ΥΔΚ που περιγράφηκε παραπάνω. Ο στόχος είναι να εκτιμηθεί το επίπεδο διακινδύνευσής της, σε πιθανή εφαρμογή της σε εθνικό επίπεδο, προκειμένου να γίνει ενοποίηση των αναγκών εξουσιοδότησης και αποφυγής αποκήρυξης ευθύνης οργανισμών που παρέχουν εφαρμογές ΗΔ για το ευρύτερο κοινό. Σχετικά παραδείγματα θα μπορούσαν να είναι οι φορολογικές υπηρεσίες του TaxisNet και ICISnet (των ΔΟΥ και Τελωνείων αντίστοιχα), υπηρεσίες ασφαλιστικών ταμείων και το δημοτολόγιο των ΟΤΑ.

Η εφαρμογή γίνεται, για λόγους συντομίας, μόνο στους κινδύνους του πολιτικού επιπέδου, ένα από τα πιο σημαντικά επίπεδα για την επιτυχία των έργων και ειδικότερα μιας δημόσιας ΥΔΚ. Σύμφωνα λοιπόν με τη μεθοδολογία RIPC^4, επιλέγονται αρχικά οι σχετικοί κίνδυνοι για τους οποίους θα γίνει η αξιολόγηση διακινδύνευσης. Για κάθε κίνδυνο υπολογίζονται η επίπτωση αν αυτός πραγματωθεί και η πιθανότητα να πραγματωθεί. Στη συνέχεια εκτιμάται η ελάχιστη κάλυψη μετρίασης, επιλέγονται οι ΚΠΕ και τα αντίμετρα που τον αφορούν και εκτιμάται το κόστος των αντιμέτρων. Μετά, υπολογίζεται η κάλυψη των αντιμέτρων που επιλέχθηκαν. Εάν υπάρχουν αλληλεξαρτήσεις με άλλους κινδύνους, κατασκευάζεται γράφος αλληλεξάρτησης και μεταβάλλονται οι πιθανότητες πραγμάτωσης των κινδύνων, βάση αυτού. Τελικά, βάση των ανωτέρω συμπληρώνεται η τελική μήτρα RIPC^4 και υπολογίζονται οι δείκτες διακινδύνευσης.

Ο Πίνακας 6 του Παραρτήματος Α είναι ένας συγκεντρωτικός πίνακας που χρησιμοποιείται για τους παραπάνω υπολογισμούς. Συγκεκριμένα, σε αυτόν παρουσιάζονται οι κίνδυνοι που αξιολογούνται στη συγκεκριμένη περίπτωση εφαρμογής και για κάθε κίνδυνο: α) τα αποτελέσματα που θα έχει στην περίπτωση πραγμάτωσής του στο έργο, από τα οποίο υπολογίζεται η τιμή της επίπτωσής του στο έργο, β) οι παράγοντες που μπορεί να προκαλέσουν την πραγμάτωσή του, οι οποίοι χρησιμοποιούνται για να υπολογιστεί η πιθανότητα πραγμάτωσής του, γ) οι τρωτότητες του έργου, που μαζί με τα

αντίμετρα χρησιμοποιούνται για να υπολογιστεί η κάλυψη των αυτών και δ) οι ΚΠΕ και τα αντίμετρα που τον αφορούν, επιλέγοντας από το υλικό της μεθοδολογίας RIPC[4].

Στο Σχήμα 16 εικονίζεται ο γράφος αλληλεξάρτησης κινδύνων για το απόσπασμα εφαρμογής της προτεινόμενης μεθοδολογίας σε μελλοντική υλοποίηση της πρωτότυπης ΥΔΚ, βάσει του γενικότερου γράφου του Σχήματος 7. Αντίστοιχα, στον Πίνακα 7 του Παραρτήματος Α παρουσιάζεται η μήτρα RIPC[4] συμπληρωμένη για τη συγκεκριμένη εφαρμογή, όπως διαμορφώνεται από τα παραπάνω δεδομένα. Οι υπολογισμοί των μετέπειτα πιθανοτήτων των κινδύνων έχουν γίνει, σύμφωνα με τις αλληλεξαρτήσεις των κινδύνων που εμφανίζονται στη στήλη «Εξάρτηση από». Μια επισκόπηση των διαφορών μεταξύ πρότερων και μετέπειτα πιθανοτήτων, δείχνει και σε αυτή την περίπτωση πόση σημασία έχει η εξάρτηση (επηρεασμός) του κινδύνου 11, για παράδειγμα από τους κίνδυνους 1 και 2, όπου οι σχετικά υψηλές πιθανότητες πραγμάτωσης των τελευταίων, αυξάνει (σημαντικά) την πιθανότητα του 11 από 0,3 σε 0,5.



Σχήμα 16. *Γράφος αλληλεξάρτησης κινδύνων για την πρωτότυπη ΥΔΚ*

Από τα δεδομένα του πίνακα, υπολογίζονται τελικά οι δείκτες αξιολόγησης, οι οποίοι έχουν ως εξής:

$Ri = 0{,}208$ $Ci = 0{,}912$

$Co = 87$ $Mi = 0{,}156$

Ερμηνεύοντας τους δείκτες, συμπεραίνεται ότι η επικινδυνότητα είναι σχετικά χαμηλή, εφόσον επιτευχθεί αποτελεσματική υλοποίηση του μεγάλου αριθμού «ακριβών» (δύσκολων για πλήρη ανάπτυξη) αντίμετρων που προτείνονται. Θα πρέπει να σημειωθεί όμως, ότι η αυτοδύναμη ερμηνεία των συγκεκριμένων αποτελεσμάτων θα είχε χαμηλό επίπεδο αξιοπιστίας. Για την αξιολόγηση ενός νέου και πρωτότυπου έργου, όπως αυτό της προτεινόμενης ΥΔΚ, τα επίπεδα στα οποία πρέπει να κινηθεί κατ' ελάχιστον η ΑΔ, για την εξαγωγή αξιόπιστων αποτελεσμάτων είναι το πολιτικό επίπεδο, το επίπεδο διοίκησης, το επίπεδο τελικού χρήστη, το νομικό/κανονιστικό επίπεδο και το οικονομικό επίπεδο.

4.3 Συμπεράσματα εφαρμογής

Στις δύο προηγούμενες ενότητες έγινε δοκιμή της προτεινόμενης μεθοδολογίας σε δύο έργα ΥΔΚ, ως κατεξοχήν έργα που απειλούνται από τους κινδύνους που πραγματεύεται η μεθοδολογία. Το ένα είναι η ΥΔΚ-ΣΥΖΕΥΞΙΣ, ένα έργο που μελετήθηκε και υλοποιήθηκε υποδειγματικά, για να μην επιτύχει όμως τελικά τους στόχους που φιλοδοξούσε σε πλάτος χώρου και βάθος χρόνου. Το έργο αυτό αποτέλεσε ένα από τα κίνητρα που οδήγησαν στην ανάπτυξη της προτεινόμενης μεθοδολογίας. Το δεύτερο έργο είναι μια πρωτότυπη ΥΔΚ που προστατεύει το απόρρητο προσωπικών πληροφοριών (ιδιοαπόρρητο) και την ελευθερία βούλησης των χρηστών της. Η αρχική επιδίωξη ήταν να αποτελέσει μια παραδειγματική περίπτωση εφαρμογής της προτεινόμενης μεθοδολογίας, διαθέτοντας όλα τα «επικίνδυνα» χαρακτηριστικά που πραγματεύεται η προτεινόμενη μεθοδολογία. Ο πρωτότυπος όμως τρόπος αντιμετώπισης της προστασίας του ιδιοαπόρρητου που εισάγει, οδήγησε σε τελικά μια υποδειγματική καθεαυτό ΥΔΚ, η οποία προτάθηκε για δημοσίευση (Kefallinos & Sykas, 2012).

Τα αποτελέσματα των δύο εφαρμογών ήταν σημαντικά για την αξιολόγηση της χρησιμότητας και της αποτελεσματικότητας της προτεινόμενης μεθοδολογίας. Συνοψίζοντας, μπορούμε να συμπεράνουμε ότι στα θετικά της μεθοδολογίας είναι ότι α) επιτυγχάνει τους στόχους της, β) αποτελεί ένα συνεκτικό, χωρίς κενά και ελλείψεις, εργαλείο, γ) είναι αποτελεσματική στην εξαγωγή συμπερασμάτων και δ) διαθέτει σημαντική ευελιξία στην εφαρμογή της. Από την άλλη μεριά όμως, απαιτεί σημαντική προσπάθεια και χρόνο για την εφαρμογή της και εξαρτάται σε σημαντικό βαθμό από την ικανότητα των αξιολογητών που την εφαρμόζουν, ώστε να παράγει χρήσιμα και με νόημα αποτελέσματα.

Η σελίδα αυτή είναι σκόπιμα λευκή

ΚΕΦΑΛΑΙΟ 5

Συζήτηση και κατευθύνσεις και περαιτέρω έρευνα και ανάπτυξη

Η σελίδα αυτή είναι σκόπιμα λευκή

Σε αυτή τη διατριβή προτάθηκε μια πρωτότυπη μεθοδολογία ΑΔ, η οποία φιλοδοξεί να διαφέρει από τις συμβατικές, στο πεδίο εφαρμογής της, στον τρόπο που εφαρμόζεται, στον τρόπο που εξάγει τα αποτελέσματα και στις μεθόδους που προτείνει για τη μείωση της επικινδυνότητας των έργων και συστημάτων που εφαρμόζεται. Αναλύθηκε το περιβάλλον της τοποθέτησής της, τα κίνητρα και η εμπειρία που ώθησαν στην ανάπτυξή της, η φιλοσοφία της, η δομή της, η διαδικασία εφαρμογής της, ο τρόπος που εξάγει τα αποτελέσματα και τα στοιχεία που χρησιμοποιεί. Για να δειχθεί ο τρόπος χρήσης της και η χρησιμότητα των αποτελεσμάτων που εξάγει, δοκιμάστηκε σε δύο έργα ΥΔΚ, ένα που έχει υλοποιηθεί και ένα που αναπτύχθηκε στο πλαίσιο της διατριβής αυτής.

Προκειμένου να είναι καλά ενημερωμένοι, διορατικοί και αποτελεσματικοί στις πρωτοβουλίες που παίρνουν, οι επαγγελματίες και ερευνητές ΗΔ πρέπει να είναι προσεκτικοί στις συναφείς προκλήσεις και κινδύνους, ενώ αναμένεται από αυτούς να χρησιμοποιούν τις κατάλληλες στρατηγικές και εργαλεία για να τους ξεπερνούν. Παρόλο που τα σύγχρονα πρότυπα ασφάλειας και διαχείρισης κινδύνου και οι αντίστοιχες μεθοδολογίες, πλαίσια και εργαλεία καλύπτουν τις διαδικασίες μοντελοποίησης ασφάλειας και τεχνικής ΑΔ πολύ καλά, θεωρούμε ότι η χρήση τους στην περιοχή έργων ΗΔ είναι υπό το βέλτιστο. Αυτό οφείλεται κυρίως στην αδυναμία να λάβουν τυπικά υπόψη κίνδυνους που πηγάζουν από μη-τεχνικά πολιτικά, οργανωτικά, κοινωνικά και ψυχολογικά θέματα της ηγεσίας και των υπαλλήλων της δημόσιας διοίκησης, διευθυντικών στελεχών, αναδόχων έργων, καθώς και του ευρύτερου κοινού.

Σε αυτό το περιβάλλον, αναπτύχθηκε η μεθοδολογία RIPC[4], η οποία στοχεύει στο να βοηθήσει τη σχεδίαση και διαχείριση συστημάτων ΗΔ πέρα από συγκεκριμένη τεχνολογία ή πλατφόρμες υλοποίησης, προς ασφαλή αποτελεσματικά και χρήσιμα συστήματα, υπηρεσίες και διαδικασίες. Καταβλήθηκε σημαντική προσπάθεια να αναλυθούν οι πραγματικοί λόγοι αποτυχίας έργων ΗΔ στη δημόσια διοίκηση και την κοινωνία, να ενσωματωθεί σημαντική εμπειρία από πολλαπλές πηγές σε αυτό τον τομέα και να προταθούν πραγματικά και αποτελεσματικά αντίμετρα και ΚΠΕ που μπορούν να βοηθήσουν στην επιτυχία των έργων.

Το κίνητρο για την ανάπτυξη της προτεινόμενης μεθοδολογίας εκπήγασε από μακρόχρονη εμπειρία και παρατήρηση στο πεδίο της ΑΔ, της ΗΔ και των έργων στον ευρύτερο δημόσιο τομέα. Σε αυτό το πεδίο, η έλλειψη διάδρασης μεταξύ των τεχνικών μεθοδολογιών (όπως και των τεχνικών εμπειρογνωμόνων και ερευνητών) και πλαισίων/προτύπων Διοίκησης Τεχνολογίας Πληροφορίας (ΔΤΠ) (και διευθυντικών/διοικητικών στελεχών), είναι συνήθης, ιδιαίτερα σε έργα όπου συμμετέχουν και

αλληλεπιδρούν δημόσιοι οργανισμοί, ο ιδιωτικός τομέας και το ευρύτερο κοινό. Από την άλλη πλευρά, η υιοθέτηση και υλοποίηση προτύπων ασφάλειας και διαδικασιών και πλαισίων ΗΔ πολλές φορές μένει στα χαρτιά και εν τέλει σπάνια βοηθά πραγματικά στην επιτυχή ολοκλήρωση των έργων. Επιπλέον, μεγάλος αριθμός σημαντικών έργων/συστημάτων αποτυγχάνουν στους στόχους τους και τη λειτουργία τους, όχι τόσο λόγω βασικών κοινωνικών εμποδίων (κάτι που επίσης συμβαίνει συχνά, παρότι στοιχειώδες), όσο λόγω βασικών ελλείψεων και εμποδίων στο άμεσο περιβάλλον υλοποίησής τους.

Σε εκ των υστέρων εφαρμογή της μεθοδολογίας σε έργα ΗΔ, βρέθηκε ότι καλύπτει ικανοποιητικά τους συνήθεις κινδύνους για την επιτυχή υλοποίηση και αποδοχή των έργων και ότι βοηθά στον αυτοέλεγχο της αξιολόγησης και στην επίγνωση των σημαντικών παραγόντων. Οι δύο εφαρμογές της μεθοδολογίας που παρουσιάστηκαν αφορούν ΥΔΚ, έργα που αποτελούν συνήθεις περιπτώσεις αποτυχίας όταν εφαρμόζονται σε μεγάλη κλίμακα, σε ιδιωτικό ή εθνικό επίπεδο, εντός και εκτός Ελλάδος. Και οι λόγοι της αποτυχίας τους (η οποία συνίσταται τυπικά σε αποτυχία διείσδυσης στο στοχευόμενο κοινό), είναι επίσης χαρακτηριστικές περιπτώσεις πραγμάτωσης των κινδύνων που αξιολογεί η προτεινόμενη μεθοδολογία. Τα αποτελέσματα των δύο εφαρμογών ήταν σημαντικά για την αξιολόγηση της χρησιμότητας και της αποτελεσματικότητας της προτεινόμενης μεθοδολογίας. Συγκεκριμένα, μπορούν να εξαχθούν τα ακόλουθα συμπεράσματα γι’ αυτήν:

α) Επιτυγχάνει τους κύριους στόχους της που είναι να οδηγήσει τους αξιολογητές σε μια συστηματική μέθοδο αξιολόγησης, να καταδείξει σημαντικούς κινδύνους που θα πρέπει να λάβουν υπόψη τους, να προτείνει αποτελεσματικά αντίμετρα προς υιοθέτηση και να εξάγει χρήσιμα αποτελέσματα εκτίμησης κινδύνου.

β) Αποτελεί ένα συνεκτικό εργαλείο και υποβοηθά τους αξιολογητές με σημαντικό υλικό για την ολοκλήρωση μιας χρήσιμης και αποτελεσματικής αξιολόγησης.

γ) Αποτελεί μια ευέλικτη μεθοδολογία που μπορεί να προσαρμοστεί σύμφωνα με την κρίση των αξιολογητών με προσθαφαίρεση στοιχείων, παραγόντων και δεδομένων σε όλα της τα δομοστοιχεία (κίνδυνοι και επίπεδα κινδύνων, ΚΠΕ, αντίμετρα, εκτίμηση επίπτωσης, παραγόντων πρόκλησης, αποτελεσμάτων πραγμάτωσης, τρωτοτήτων, ενδεχομένων αντίστροφης πραγμάτωσης). Με αλλαγή στους κίνδυνους, στους ΚΠΕ και τα αντίμετρα μπορεί να εφαρμοστεί ακόμα και σε άλλα πεδία ΑΔ.

δ) Με προσοχή στην εξαγωγή συμπερασμάτων μπορούν να αξιολογηθούν ακόμα και μεμονωμένα επίπεδα διακινδύνευσης του υπό εξέταση έργου/συστήματος.

ε) Όπως όλες οι μεθοδολογίες ΑΔ, εξαρτάται σε σημαντικό βαθμό από την ικανότητα των αξιολογητών που την εφαρμόζουν, ώστε να παράγει χρήσιμα αποτελέσματα με νόημα.

στ) Όπως όλες οι μεθοδολογίες ΑΔ, απαιτεί σημαντική προσπάθεια και χρόνο για την αναλυτική εφαρμογή της. Αυτό μπορεί να μειωθεί σε αρκετό βαθμό αν γίνει προσεγγιστική ή/και κατ' εκτίμηση τοποθέτηση των πιθανοτήτων πραγμάτωσης των κινδύνων, των επιπτώσεών τους και της κάλυψης των αντιμέτρων (για όλα ή για κάποια από αυτά) και όχι ο αναλυτικός υπολογισμός που περιγράφεται. Και πάλι, αυτό εξαρτάται από την κρίση, την εμπειρία και ικανότητα των αξιολογητών που την εφαρμόζουν.

Επομένως, η προτεινόμενη μεθοδολογία ΑΔ μπορεί να αποτελέσει αποτελεσματικό αρωγό για την επιτυχία των έργων, με το μοναδικό μειονέκτημα, λόγω της (προς το παρόν) μη υλοποίησης της σε λογισμικό, μιας σχετικά χρονοβόρας διαδικασίας εφαρμογής. Η καινοτομία της προσέγγισής της βρίσκεται:

α) Στην ενσωμάτωση μεγάλου αριθμού μη συμβατικών και μη τεχνικών παραγόντων κινδύνου, αλλά σχετικών με την ΗΔ και συχνά εμφανιζόμενων, από περιοχές όπως η κοινωνία, οι τελικοί χρήστες, η δημόσια διοίκηση, οι πολιτική, το νομικό και κανονιστικό πλαίσιο, ακόμα και η ψυχολογία, σε μια εύκολη στη χρήση επαναληπτική διαδικασία ΑΔ.

β) Στην εξαγωγή αποτελεσμάτων με χρήση πρακτικών, δεκτικών σε συγκριτικές διαδικασίες και περιληπτικών δεικτών διακινδύνευσης.

γ) Στη διαφορετική προσέγγισή της στην ΑΔ συστημάτων και έργων ΗΔ. Ακολουθώντας διαφορετική φιλοσοφία από τις συμβατικές τεχνικές μεθοδολογίες και εργαλεία (τα οποία προσανατολίζονται περισσότερο προς τις τεχνικές λεπτομέρειες), ενσωματώνει ειδικότερα περιοχές διακινδύνευσης ιδιαίτερα σημαντικές στο πεδίο των έργων ΗΔ, οι οποίες αποτελούν πιο συνήθεις λόγους αποτυχίας των. Αποτελεί έτσι μια διεπαφή ανάμεσα στην ευρύτερη τεχνοκρατική διοικητική φιλοσοφία των COBIT, ISO/IEC 27002 και ITIL και των τεχνικών μεθοδολογιών ΑΔ, προσθέτοντας και αναδεικνύοντας νέες διαστάσεις, στις οποίες πρέπει να κατευθυνθεί η προσοχή προσώπων-κλειδιά έργων ΗΔ, έτσι ώστε να κινήσουν τις αντίστοιχες δράσεις και να λάβουν τα απαραίτητα μέτρα.

δ) Στην προαγωγή του αυτοέλεγχου και της αυτοαξιολόγησης της διαδικασίας ΑΔ, πέρα από τα όρια των τεχνικών εργαλείων και εντός της περιοχής των πλαισίων ΔΤΠ και των αποτελεσματικών πρακτικών ΗΔ.

ε) Στη μεγάλη ευελιξία. Οι αξιολογητές μπορούν να επιλέξουν (και να προσθαφαιρέσουν) από τα στοιχεία που παρέχει η μέθοδος αυτά που επιθυμούν, χωρίς να επηρεάζεται η δυνατότητά της να εξάγει αποτελέσματα. Ασφαλώς, όσο πιο πλήρη είναι τα στοιχεία που θα επιλεγούν, όσο καλύτερα καλύπτουν την περίπτωση εφαρμογής, τόσο πιο αξιόπιστα θα είναι τα αποτελέσματα. Ωστόσο οι αξιολογητές μπορούν να επιλέξουν τους κινδύνους που θα αξιολογήσουν, τα αποτελέσματά τους σε περίπτωση πραγμάτωσης, τους παράγοντες που μπορεί να τους προκαλέσουν, τις τρωτότητες του έργου που μπορεί να αποτελέσουν σημεία τρώσης και από αυτές την κάλυψη των αντιμέτρων. Η προτεινόμενη μεθοδολογία επομένως διαθέτει την ευελιξία για να εφαρμοστεί σαν σχεδιότυπο ουσιαστικά σε οποιοδήποτε είδος συστήματος, σε οποιοδήποτε τομέα ΑΔ.

Οι παράγοντες που επηρεάζουν την επιτυχή εφαρμογή και την εξαγωγή ορθών αποτελεσμάτων της ίδιας της μεθοδολογίας συνίστανται:

α) Στην επιλογή όλων των σημαντικών για το έργο κινδύνων, ακόμα και πέρα, αν απαιτείται, από αυτούς που προτείνονται, σύμφωνα με την κρίση των αξιολογητών.

β) Στη συμπερίληψη των απαραίτητων για τους σκοπούς του έργου κρίσιμων παραγόντων επιτυχίας (ΚΠΕ), και

γ) Στην επιλογή αποτελεσματικών, εφικτών και οικονομικά αποδοτικών αντιμέτρων που δεν αποβαίνουν σε βάρος της λειτουργικότητας και της φιλικότητας του συστήματος.

Η κύρια αδυναμία της μεθοδολογίας, στην τρέχουσα μορφή της, είναι ότι η απόδοση και η αποτελεσματικότητά της εξαρτάται από την αποφασιστικότητα, τη διορατικότητα και την εμπειρία των επαγγελματιών που θα το χρησιμοποιήσουν (κάτι που ισχύει ούτως ή άλλως για όλες τις μεθοδολογίες και εργαλεία ΑΔ), μαζί με άλλα περισσότερο καθιερωμένα εργαλεία. Αυτό διότι, αν και αποτελεί ένα ολοκληρωμένο εργαλείο με πλήρεις βιβλιοθήκες στοιχείων, δεν είναι στην τρέχουσα μορφή του υλοποιημένο σε λογισμικό, έτσι ώστε πλήρως αυτόνομα να μπορεί να εξασφαλίσει λεπτομερή προσέγγιση της ασφάλειας, συστηματική αξιολόγηση των υποστοιχείων των έργων και ολοκληρωμένη τεκμηρίωση των πολιτικών και των μέτρων που πρέπει να εφαρμοστούν.

Η ανάπτυξη της μεθοδολογίας σε λογισμικό, με βάση γνώσης για τους κινδύνους, τους ΚΠΕ και τα αντίμετρα, έτοιμα εργαλεία κατασκευής γράφων αλληλεξαρτήσεων, υπολογισμού των πιθανοτήτων και αναφορών, καθώς και διεπαφές με εμπορικά συστήματα ΑΔ θα αποτελέσει αντικείμενο περαιτέρω εξέλιξης με σκοπό την εμπορική εκμετάλλευση.

Ως αντικείμενο περαιτέρω έρευνας προτείνεται η διαμόρφωση της μεθοδολογίας σε σχεδιότυπο για εφαρμογή σε άλλα πεδία εφαρμογής ΑΔ. Προσαρμόζοντας τις περιοχές κινδύνου, τους ΚΠΕ και τα αντίμετρα, ο αλγόριθμος και οι δείκτες της μεθοδολογίας μπορούν να εφαρμοστούν κατάλληλα, ώστε να αποτελέσουν χρήσιμο εργαλείο και σε άλλους τομείς, τεχνολογικούς και μη, όπως βιολογικά συστήματα, οικοσυστήματα, κοινωνικές δομές κ.ά.

Η σελίδα αυτή είναι σκόπιμα λευκή

ΠΑΡΑΡΤΗΜΑ Α

Πίνακες στοιχείων εργαλείου αξιολόγησης διακινδύνευσης και εφαρμογών του

Η σελίδα αυτή είναι σκόπιμα λευκή

Πίνακας 2. *Κίνδυνος – ΚΠΕ – Αντίμετρα*

ΚΠΕ και αντίμετρα, που προτείνονται σαν μέρος του εργαλείου εφαρμογής ΑΔ που συνοδεύει τη μεθοδολογία RIPC[4].

Α/Α	**Κίνδυνος**	**ΚΠΕ**	**Αντίμετρα**
Α	***Πολιτικό Επίπεδο***		
1	Υποστηριχτική αποφασιστικότητα και λήψη αποφάσεων	Η πολιτική ηγεσία πιστεύει στο έργο και στη συμβολή του στο δημόσιο συμφέρον και την ΗΔ και είναι ενήμερη για τον απαιτούμενο χρονισμό και τη φύση των αποφάσεων και των βημάτων που απαιτούνται για την επιτυχία του έργου. Η εμπιστοσύνη και η υποστήριξη στο έργο είναι σταθερή και διακομματική ή/και επιβάλλεται από διεθνείς παράγοντες.	Βολιδοσκόπηση και αξιολόγηση των προθέσεων και των κινήτρων της πολιτικής ηγεσίας, επικοινώνηση των στόχων, των προτερημάτων, των πιθανών αποτελεσμάτων, των εμποδίων και των πιθανοτήτων επίτευξης των στόχων του έργου προς την πολιτική ηγεσία, παροχή κατάλληλων κινήτρων και επιχειρημάτων στην πολιτική ηγεσία, προς όφελος του έργου.
2	Μεσο/μακρο-πρόθεσμος ενιαίος σχεδιασμός και δέσμευση στο έργο (πολιτικό επίπεδο)	Η πολιτική ηγεσία είναι διαχρονικά ενήμερη για τις φάσεις, την κατάσταση, τα προαπαιτούμενα, το χρονισμό, τη φύση των αποφάσεων και των βημάτων που απαιτούνται για την επιτυχία του έργου του έργου. Η εμπιστοσύνη και η υποστήριξη στο έργο είναι διακομματική ή/και επιβάλλεται από διεθνείς παράγοντες. Το έργο είναι ενταγμένο στο μεσο/μακρο-πρόθεσμο κυβερνητικό σχεδιασμό, ο οποίος δεν μεταβάλλεται από κυβέρνηση σε κυβέρνηση.	Διαρκής ενημέρωση της πολιτικής ηγεσίας για τις φάσεις, την κατάσταση, τα προαπαιτούμενα, το χρονισμό και τη φύση των αποφάσεων και των βημάτων που απαιτούνται για την επιτυχία του έργου, καθώς και των επιπτώσεων της αποτυχίας. Προβολή των ωφελημάτων του έργου σε κυβερνητικό, εθνικό, κομματικό και διακομματικό επίπεδο. Προβολή των τεχνολογιών του έργου ως μέσο προώθησης της κυβερνητικής πολιτικής και βελτίωσης της εικόνας του κυβερνητικού έργου. Παροχή κινήτρων και επιχειρημάτων για την υποστήριξη του έργου, λόμπυινγκ (προώθηση) για το έργο. Όπου το έργο σχετίζεται με διεθνείς συνθήκες ή/και χρηματοδότηση, ενημέρωση της ηγεσίας για τις συνέπειες μη ολοκλήρωσης και χρήση του διεθνούς παράγοντα ως μόχλευση για την προώθηση του έργου. Ειδική πρόβλεψη για τη συνέχιση της υποστήριξης, της υλοποίησης και της λειτουργίας του έργου μετά

			από αλλαγή κυβέρνησης. Πρόβλεψη για την ένταξη του έργου στον κυβερνητικό σχεδιασμό και παροχή των προαπαιτούμενων γι' αυτό.
3	Κοινωνική και εμπορική τοποθέτηση και αιτιολόγηση (πόσο καλά τοποθετείται το έργο για να ανταποκριθεί και να καλύψει κοινωνικές και εμπορικές ανάγκες)	Το έργο τοποθετείται και λειτουργεί κατάλληλα και επαρκώς για να καλύψει υπάρχουσες κοινωνικές και εμπορικές ανάγκες, με την υποστήριξη της πολιτικής ηγεσίας. Η ολοκλήρωσή του φτάνει σε σημείο λειτουργικότητας και διάθρωσης ώστε να καλύπτει πραγματικούς σκοπούς, ανάγκες και απαιτήσεις.	Καθοδήγηση, έλεγχος και αξιολόγηση, πριν, κατά και μετά την ολοκλήρωση του έργου έτσι ώστε να εξασφαλίζονται οι απαιτήσεις τοποθέτησης και λειτουργίας του. Έρευνα σε στοχευόμενους χρήστες και μη, χρησιμότητας και τοποθέτησης του έργου, τόσο κατά τη φάση δοκιμαστικής λειτουργίας, όσο και στη κανονική λειτουργία του. Χρήση διαδραστικών τεχνολογιών ενημέρωσης, ηλεκτρονικής διακυβέρνησης, ΜΜΕ και δημοσκοπήσεων.
4	Υποστήριξη για/από άλλες συμπληρωματικές ή ακολουθιακές πολιτικές και έργα (πολιτικό επίπεδο)	Το έργο είναι τοποθετημένο σε πολιτικό και λειτουργικό περιβάλλον ευνοϊκό για την ολοκλήρωση και λειτουργία του και πλαισιώνεται από άλλα έργα που το συμπληρώνουν και το υποστηρίζουν. Τα έργα αυτά ολοκληρώνονται σύμφωνα με τις απαιτήσεις του υπό εξέταση έργου, έτσι ώστε να μην δημιουργούν εμπόδια.	Προώθηση κεντρικού πολιτικού σχεδιασμού που ευνοεί το υπό εξέταση έργο, κατανόηση και υπόδειξη των εξαρτήσεων του έργου από πολιτικές και άλλα έργα, προώθηση της επίτευξης των στόχων των υπό εξάρτηση έργων. Πρόβλεψη για αντιμετώπιση απρόβλεπτων/έκτακτων καταστάσεων.
5	Κουλτούρα τεχνολογίας της πολιτικής ηγεσίας	Η πολιτική ηγεσία διαθέτει τεχνολογική αίσθηση και άποψη, κατανοεί την τεχνολογική διάσταση του έργου, συνδέει την τεχνολογική με την πολιτική/κοινωνική διάσταση και χρησιμότητα του έργου	Επιμόρφωση και ενημέρωση της πολιτικής ηγεσίας, λόμπυινγκ (προώθηση) για το έργο, χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης, υποστήριξη από τα ΜΜΕ.
6	Εξοικείωση της πολιτικής ηγεσίας με το έργο (σε υψηλό επίπεδο)	Η πολιτική ηγεσία διαθέτει επαρκή γνώση για τη πολιτική, κοινωνική, επιχειρηματική, οικονομική και τεχνολογική χρησιμότητα του έργου, τις τεχνολογίες που εισάγει (σε υψηλό επίπεδο), καθώς και των απαιτήσεων για την ολοκλήρωση και την επίτευξη των στόχων του.	Κατάλληλη επιμόρφωση και ενημέρωση της πολιτικής ηγεσίας, λόμπυινγκ (προώθηση) για το έργο, κατανόηση και υπόδειξη των εξαρτήσεων του έργου από πολιτικές και άλλα έργα, προώθηση των τεχνολογιών του έργου ως μέσο προώθησης της κυβερνητικής πολιτικής και βελτίωσης της εικόνας του κυβερνητικού έργου.
7	Επαρκής και διαχρονική κατανομή πιστώσεων (υψηλό στρατηγικό επίπεδο)	Το έργο διαθέτει διαχρονικά τις απαραίτητες πιστώσεις για την ολοκλήρωσή του και την επίτευξη των στόχων του.	Όπου αυτό εξαρτάται από εθνικές συνθήκες, έγκαιρος προγραμματισμός και προϋπολογισμός· όπου εξαρτάται

			από διεθνείς συνθήκες, κατάλληλη ανταπόκριση στα εθνικά προαπαιτούμενα και επικοινώνηση της κατάστασης ανάπτυξης και ολοκλήρωσης του έργου.
8	Κατανομή αρμοδιότητας/δικαιοδοσίας μεταξύ κυβερνητικών υπηρεσιών	Έχει εκχωρηθεί, νομικά, κανονιστικά ή διοικητικά στους φορείς που μετέχουν στα στάδια του έργου η κατάλληλη δικαιοδοσία, χωρίς να παρουσιάζονται εμπόδια από άλλους φορείς.	Έγκαιρη επικοινώνηση προς την πολιτική ηγεσία των αναγκών δικαιοδοσίας των φορέων που μετέχουν στο έργο, προκειμένου να ρυθμιστούν κατάλληλα τα νομικά, κανονιστικά και διοικητικά πλαίσια. Πρόβλεψη για μηχανισμό και διαδικασίες ταχείας αντιμετώπισης και επίλυσης στην περίπτωση που εμφανίζονται προβλήματα δικαιοδοσίας.
9	Τοποθέτηση και αλληλεπίδραση με/εντός εθνικών πολιτικών και βραχυ/μεσοπρόθεσμων εθνικών στρατηγικών (πολιτικό επίπεδο)	Το έργο είναι σύμφωνο και αλληλεπιδρά θετικά με εθνικές πολιτικές και στρατηγικές και είναι ανθεκτικό σε αλλαγές αυτών, διότι ανταποκρίνεται σε διαχρονικές, πραγματικές εθνικές, κοινωνικές, οικονομικές ανάγκες.	Σωστός επιχειρηματικός, πολιτικός, οικονομικός και κοινωνικός σχεδιασμός του έργου, ευελιξία των στόχων και των απαιτήσεών του σε μεταβλητό πολιτικό και εθνικό περιβάλλον, σωστή επικοινωνία και λόμπυινγκ του έργου προς την ηγεσία. Προσαρμογή των εθνικών πολιτικών και στρατηγικών, όπου αυτό είναι δυνατό.
10	Τοποθέτηση και αλληλεπίδραση του έργου με περιφερειακές και κεντρικές διεθνείς οδηγίες, πολιτικές και έργα (πολιτικό επίπεδο)	Το έργο είναι σύμφωνο και αλληλεπιδρά θετικά με διεθνείς περιφερειακές και κεντρικές πολιτικές, στρατηγικές, οδηγίες και έργα και είναι ανθεκτικό σε αλλαγές αυτών, διότι ανταποκρίνεται σε διαχρονικές, πραγματικές εθνικές και διεθνείς ανάγκες.	Σωστός επιχειρηματικός σχεδιασμός του έργου σε σχέση με άλλα διεθνή έργα, ευελιξία των στόχων και των απαιτήσεών του σε μεταβλητό πολιτικό και εθνικό περιβάλλον, σωστή επικοινωνία και λόμπυινγκ του έργου.
11	Παρουσίαση, αιτιολόγηση και προώθηση του έργου στο προσωπικό κατώτερου κυβερνητικού/διοικητικού επιπέδου, στα ΜΜΕ και το ευρύ κοινό (πολιτικό επίπεδο)	Με ενέργειες της ηγεσίας, το έργο είναι γνωστό και κατανοητό, όσον αφορά τους στόχους του, τις ανάγκες, τα στάδια, τη χρησιμότητα και την κατάστασή του, στο κατώτερο κυβερνητικό και διοικητικό προσωπικό και στο ευρύ κοινό	Διαχρονική υποστήριξη του έργου από την πολιτική ηγεσία, κατάλληλη επικοινώνηση και προώθησή του με τρόπο που να αφομοιώνεται εύκολα από το κατώτερο κυβερνητικό/διοικητικό επίπεδο και το ευρύ κοινό. Χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης. Ειδικά για τα ΜΜΕ, προσέγγιση και προβολή του έργου με κατάλληλο τρόπο, γειτνίασή του με τα συμφέροντά τους, ένταξή του στη γενικότερη προωθη-

			τική προσπάθεια της κυβέρνησης, δημιουργία κινήτρων και αναγκών στους χρήστες (εφόσον τα πραγματικά δεν επαρκούν/υπάρχουν) μέσω των ΜΜΕ.
12	Οικονομικές, διοικητικές και διαπροσωπικές σχέσεις (όπου σχετίζονται και μπορούν να επηρεάσουν το έργο) με τοπικές και εθνικές οικονομικές και παραγωγικές δυνάμεις, εθνικά/τοπικά ΜΜΕ	Τοπικές και εθνικές οικονομικές και παραγωγικές δυνάμεις, όπως και τοπικά και εθνικά ΜΜΕ βλέπουν ωφελήματα από το έργο, είτε από την ανάπτυξή του είτε από τα αποτελέσματά του, είτε άμεσα, είτε έμμεσα, μέσω άλλων έργων.	Σωστή τοποθέτηση και επιχειρηματική σχεδίαση του έργου, λόμπυινγκ στους κατάλληλους παράγοντες και ΜΜΕ, παρουσίαση με τρόπο ώστε να κάνει το έργο απαραίτητο στη συνείδηση και στα συμφέροντά τους.
13	Οικονομικές, διοικητικές και πολιτικές σχέσεις και συνθήκες (που σχετίζονται και μπορούν να επηρεάσουν το έργο) με γειτονικές, περιφερειακές και κεντρικές κυβερνητικές, οικονομικές και παραγωγικές δυνάμεις, διεθνή ΜΜΕ	Γειτονικές, περιφερειακές ή κεντρικές κυβερνητικές, οικονομικές ή παραγωγικές δυνάμεις και ΜΜΕ βλέπουν ωφελήματα από το έργο, είτε από την ανάπτυξή του είτε από τα αποτελέσματά του, είτε άμεσα, είτε έμμεσα, μέσω άλλων έργων.	Σωστή τοποθέτηση και επιχειρηματική σχεδίαση του έργου, λόμπυινγκ στους κατάλληλους παράγοντες και ΜΜΕ, παρουσίαση με τρόπο ώστε να κάνει το έργο απαραίτητο στη συνείδηση και στα συμφέροντά τους.
14	Πρόβλεψη, διασφάλιση και παρακολούθηση αποτελεσματικότητας ως προς την παροχή κινήτρων για την ορθή και υπεύθυνη υλοποίηση, λειτουργία και χρήση του έργου, προς τη διοίκηση, τους αναδόχους/εργολάβους, το προσωπικό υπηρεσίας και το κοινό στο οποίο απευθύνεται (πολιτικό επίπεδο)	Με πρωτοβουλία της πολιτικής ηγεσίας, η διοίκηση, οι ανάδοχοι/εργολάβοι, το προσωπικό υπηρεσίας και το κοινό στο οποίο απευθύνεται το έργο έχουν τα κατάλληλα κίνητρα και κατανόηση ώστε να διοικήσουν, υλοποιήσουν, λειτουργήσουν και χρησιμοποιήσουν, αντίστοιχα, σωστά το έργο, προκειμένου να επιτύχει τους στόχους του και να έχει τα αναμενόμενα θετικά αποτελέσματα, τα οποία θα έχουν με τη σειρά τους θετικό αντίκτυπο στη γνώμη που έχουν οι παραπάνω για την πολιτική ηγεσία (κλείσιμο κύκλου). Κατανόηση από την ηγεσία των κινήτρων που πρέπει να έχουν οι υπόλοιποι προς όφελος του έργου.	Παροχή κατάλληλων κινήτρων στην πολιτική ηγεσία για διαχρονική υποστήριξη και προώθηση του έργου, με απώτερο στόχο η επιτυχία του να έχει θετικό αντίκτυπο στη γνώμη των υπολοίπων προς αυτή. Καλλιέργεια της κατάλληλης εργοστραφούς κουλτούρας της ηγεσίας. Επικοινώνηση των κινήτρων που πρέπει να έχει το κατώτερο προσωπικό και το ευρύ κοινό προς όφελος της επίτευξης των στόχων και της ορθής λειτουργίας του έργου.
Β	***Επίπεδο Διοίκησης***		
15	Βραχυ/μεσο-πρόθεσμος ενιαίος σχεδιασμός και δέσμευση στο έργο (επίπεδο	Η διοίκηση είναι διαχρονικά ενήμερη για τις φάσεις, την κατάσταση, τα προαπαιτούμενα, το χρονισμό, τη φύση	Διαρκής ενημέρωση της διοίκησης για τις φάσεις, την κατάσταση, τα προαπαιτούμενα, το χρονισμό και τη φύση

	διοίκησης)	των αποφάσεων και των βημάτων που απαιτούνται για την επιτυχία του έργου του έργου. Η διοίκηση έχει τα κίνητρα για την σταθερή υποστήριξη του έργου, τα οποία δεν εστιάζονται σε συγκεκριμένα άτομα, αλλά είναι διαχρονικά.	των αποφάσεων και των βημάτων που απαιτούνται για την επιτυχία του έργου, καθώς και των επιπτώσεων της αποτυχίας. Παροχή κινήτρων και επιχειρημάτων για την υποστήριξη του έργου, λόμπυινγκ (προώθηση) για το έργο, ημερίδες και σεμινάρια προσανατολισμένα προς το διοικητικό προσωπικό, διασφάλιση ότι η υποστήριξη του έργου από την πολιτική ηγεσία δρα θετικά, ενώ η απουσία της δεν δρα αρνητικά. Πρόβλεψη και λειτουργία διαδικασιών άμεσης αντιμετώπισης προβλημάτων.
16	Επαρκής σχεδίαση και αιτιολόγηση επιχειρηματικής περίπτωσης (business case development)	Η διοίκηση των οργανισμών που εμπλέκονται στο έργο διαθέτουν πλήρες επιχειρηματικό σχέδιο και αιτιολόγηση για το έργο (και τα αποδέχονται ως ορθά), έτσι ώστε να διαθέτουν τα εργαλεία για την υποστήριξη και προώθησή του σε ανώτερα και κατώτερα κλιμάκια. Το έργο ταιριάζει με το περιβάλλον του και οι στόχοι του έρχονται να ικανοποιήσουν πραγματικές ανάγκες, προς όφελος του κοινού που απευθύνεται και των φορέων που το υλοποιούν. Η επιχειρηματική περίπτωση ταιριάζει με την οικονομική μελέτη, σκοπιμότητα, στόχους και περιβάλλον του έργου.	Εκπόνηση και αιτιολόγηση ορθού και πλήρους επιχειρηματικού σχεδίου, με διαδικασίες αυτοαξιολόγησης και ενημέρωσης, έτσι ώστε το έργο να μπορεί να ανταποκριθεί στις συνθήκες του περιβάλλοντός του (που μπορεί να μεταβάλλονται) και να ανταποκρίνεται σε πραγματικές ανάγκες, προς όφελος του κοινού και των φορέων που το υλοποιούν. Μελέτη σκοπιμότητας και διαβούλευση με ενδιαφερόμενους/εξαρτώμενους φορείς/ομάδες/κοινό, καθώς και οικονομικές υπηρεσίες. Επικοινώνηση της επιχειρηματικής περίπτωσης προς την πολιτική ηγεσία, προς εξασφάλιση διαρκούς υποστήριξης και κεφαλαίων.
17	Κατάλληλη και πλήρης σχεδίαση και επίβλεψη της στρατηγικής εκτέλεσης του έργου	Η διοίκηση διαθέτει το σχέδιο, τις γνώσεις, τη δικαιοδοσία και τα κίνητρα για να επιβλέψει τη στρατηγική και τη μέθοδο για την ορθή και πλήρη εκτέλεση του έργου.	Εκπόνηση στρατηγικού σχεδίου/μεθόδου/διαδικασίας για την ορθή και πλήρη εκτέλεση του έργου, η οποία θα προβλέπει και θα αντιμετωπίζει ενδεχόμενα προβλήματα. Εκπόνηση και εφαρμογή διαδικασιών επίβλεψης της υλοποίησης του έργου. Παροχή κινήτρων στη διοίκηση για την ορθή επίβλεψη και ολοκλήρωση του έργου. Πρόβλεψη και λειτουργία διαδικασιών άμεσης αντιμετώπισης προβλημάτων.
18	Λειτουργική, στόχο-προσανατολισμένη,	Το έργο διαθέτει πλήρη, άρτια, σύγχρονα και πραγματο-	Σύνταξη πλήρων, τεχνολογικά άρτιων, σύγχρονων, πραγ-

	με τεχνολογική επίγνωση και φιλική προς το χρήστη σύνταξη και επίβλεψη χαρακτηριστικών του έργου	ποιήσιμα χαρακτηριστικά, το οποία ακολουθούνται, όσον αφορά την υλοποίηση, από την επιτροπή παρακολούθησης και παραλαβής και εφαρμόζονται από τους αναδόχους, με τελικό σκοπό την επίτευξη των στόχων και την ολοκλήρωση του έργου.	ματοποιήσιμων και φιλικών προς τον ανάδοχο και το χρήστη χαρακτηριστικών για το έργο. Διασφάλιση ότι η αντικειμενικότητα των χαρακτηριστικών, σε σχέση με κατασκευαστές και αναδόχους, δεν γίνεται εις βάρος των παραπάνω, όπως επίσης ως προς τους στόχους και τη λειτουργικότητα του έργου. Σύνταξη και διασφάλιση λειτουργίας ορθών διαδικασιών επίβλεψης και ελέγχων για την εφαρμογή των χαρακτηριστικών.
19	Τεχνολογική κουλτούρα του διοικητικού προσωπικού	Το προσωπικό διοίκησης είναι θετικά προσανατολισμένο και ενημερωμένο στις σχετικές με το έργο τεχνολογίες και δεν έχει αίσθημα αποστροφής προς αυτές.	Ημερίδες παρουσίασης και ενημέρωσης, σεμινάρια και προγράμματα εκπαίδευσης προσανατολισμένα προς το διοικητικό προσωπικό, ενεργή συμμετοχή του διοικητικού προσωπικού στον τεχνικό σχεδιασμό και την παρακολούθηση έργων, χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.
20	Εξοικείωση του διοικητικού προσωπικού με το έργο	Το προσωπικό διοίκησης είναι θετικά ενημερωμένο για τους στόχους, τις μεθόδους, τις διαδικασίες και την τρέχουσα κατάσταση του έργου, καθώς και με τις σχετικές με αυτό τεχνολογίες.	Ημερίδες παρουσίασης και ενημέρωσης, σεμινάρια και προγράμματα εκπαίδευσης προσανατολισμένα προς το διοικητικό προσωπικό, ενεργή συμμετοχή του διοικητικού προσωπικού στον τεχνικό σχεδιασμό και την παρακολούθηση του έργου, παροχή κινήτρων για την εξοικείωση με το έργο, κανάλια επικοινωνίας και αναφοράς για την τρέχουσα κατάσταση του έργου, χρήση διαδραστικών τεχνολογιών ενημέρωσης, διοίκησης, παρακολούθησης έργων και ηλεκτρονικής διακυβέρνησης.
21	Νομική, κανονιστική, πολιτική (policy) και διαδικαστική προσαρμογή προς το έργο και συμμόρφωση από το έργο	Το νομικό, κανονιστικό, πολιτικό και διαδικαστικό περιβάλλον του έργου είναι ευνοϊκό προς αυτό και δεν του θέτει εμπόδια ως προς την επίτευξη των στόχων, την ολοκλήρωση και την εύρυθμη λειτουργία του.	Έγκαιρη ανάλυση και εκτίμηση κινδύνων, ενημέρωση και αντιμετώπιση δυσκολιών και εμποδίων, όσον αφορά το νομικό, κανονιστικό, πολιτικό και διαδικαστικό περιβάλλον του έργου, με προώθηση λήψης των απαιτούμενων δράσεων από την πολιτική και διοικητική ηγεσία των φορέων που εμπλέκονται. Ο κατάλληλος χρονικός σχεδια-

			σμός και πρόβλεψη αποτελεί πρωτεύων παράγοντα. Πρόβλεψη και λειτουργία διαδικασιών άμεσης αντιμετώπισης προβλημάτων.
22	Αρμόζουσα εκχώρηση αρμοδιοτήτων και εξουσίας στην ιεραρχία διακυβέρνησης και διοίκησης	Οι φορείς και οι παράγοντες που εμπλέκονται στην υλοποίηση και τη λειτουργία του έργου διαθέτουν καλώς ορισμένες αρμοδιότητες, τόσο σε οριζόντιο, όσο και σε κάθετο επίπεδο για την επίτευξη των στόχων, την ολοκλήρωση και την εύρυθμη λειτουργία του έργου.	Ανάλυση απαιτήσεων αρμοδιότητας και εκτίμησης συγκρούσεων, προγραμματισμός και ανάληψη δράσεων για την έγκαιρη και αποτελεσματική εκχώρηση αρμοδιοτήτων στους φορείς που εμπλέκονται, από την διοικητική και πολιτική ηγεσία. Ενημέρωση πολιτικής και διοικητικής ηγεσίας. Πρόβλεψη και λειτουργία διαδικασιών άμεσης αντιμετώπισης προβλημάτων.
23	Αιτιολόγηση κόστους, ολικά, μερικά και κατά στάδια και δομοστοιχεία	Το έργο διαθέτει, από την πλευρά της διοίκησης, ανάλυση κόστους για όλα τα στάδια και τα δομοστοιχεία του, προκειμένου να είναι εξασφαλισμένη η έγκαιρη και επαρκής χρηματοδότησή του, τουλάχιστον όσον αφορά την επικοινώνηση αυτών στις οικονομικές υπηρεσίες.	Λήψη δράσεων από την διοίκηση για κατάλληλη και επαρκή κατανομή πιστώσεων και επικοινώνηση αυτών προς/από την αρμόδια οικονομική υπηρεσία. Συνεργασία διοικητικών φορέων με οικονομικές αρχές, φορείς και παράγοντες για την επαρκή χρηματοδότηση του έργου και ικανοποίηση των προαπαιτήσεων για αυτήν.
24	Μεθοδολογία διασφάλισης παραγωγικότητας, παρακολούθησης προόδου και απόδοσης ευθύνης	Η παραγωγικότητα και η αποτελεσματικότητα του προσωπικού των φορέων και των αναδόχων διασφαλίζεται από σύστημα αξιολόγησης, παρακολούθησης και απόδοσης ευθύνης. Το έργο χρησιμοποιεί τους ανθρώπινους, τεχνολογικούς και οικονομικούς πόρους του με κατά το δυνατόν βέλτιστο τρόπο για την επίτευξη των στόχων και την εύρυθμη λειτουργία του.	Ανάπτυξη ή χρησιμοποίηση πιστοποιημένης μεθοδολογίας παρακολούθησης και διασφάλισης παραγωγικότητας, προόδου και απόδοσης ευθύνης, έτσι ώστε το έργο χρησιμοποιεί τους ανθρώπινους, τεχνολογικούς και οικονομικούς πόρους του με κατά το δυνατόν βέλτιστο τρόπο, για την επίτευξη των στόχων και την εύρυθμη λειτουργία του. Επικοινώνηση των αποτελεσμάτων στην διοικητική και πολιτική ηγεσία, αυτοαξιολόγηση της μεθοδολογίας και εφαρμογή με επαναληπτικό τρόπο σε όλα τα στάδια του έργου.
25	Τεχνολογική, διαδικαστική και διοικητική ετοιμότητα εταίρων (εξωτερικών οργανισμών)	Οι εξωτερικοί των φορέων του έργου οργανισμοί βρίσκονται σε ετοιμότητα και ενημέρωση ώστε να υποβοηθήσουν το έργο, να ικανοποιήσουν τα προαπαιτούμενα και	Εκστρατεία ενημέρωσης και εξοικείωσης των εξωτερικών φορέων με το έργο, σχεδιασμός, εφαρμογή και αξιολόγηση διαδικασιών ενημέρωσης και διαπροσωπείας με τους

		να παρέχουν βέλτιστη πληροφόρηση και την υποστήριξη προς όφελος του έργου. Πίστη των εξωτερικών φορέων στους στόχους και τη χρησιμότητα του έργου και σε αμοιβαίο όφελος	εξωτερικούς φορείς, συμμετοχή αυτών, έστω και ενημερωτικά, στις διαδικασίες όλων των σταδίων του έργου, διασφάλιση κατάλληλου χρονισμού ενημέρωσης και δράσεων για την υποστήριξη του έργου και την ικανοποίηση των προαπαιτούμενων αυτού.
26	Υποστήριξη για / από άλλες συμπληρωματικές ή ακολουθιακές πολιτικές και έργα (επίπεδο διοίκησης)	Το έργο ταιριάζει μέσα σε ευρύτερο πλαίσιο έργων και στρατηγικών για την προώθηση και ανάπτυξη της ΗΔ και των στόχων του ευρύτερου χώρου των οργανισμών στους οποίους θα υλοποιηθεί. Άλλα έργα και πολιτικές που ακολουθούνται δρουν υποστηρικτικά για το έργο.	Σωστή σχεδίαση επιχειρηματικής περίπτωσης του έργου, πρόβλεψη και υλοποίηση υποστηρικτικών δράσεων, προσαρμογή πολιτικών και στρατηγικών όπου απαιτείται, προσαρμογή της σχεδίασης, προγραμματισμού, υλοποίησης και λειτουργίας του έργου, όπου αυτά δεν ταιριάζουν με τις πολιτικές και άλλα έργα του περιβάλλοντός του.
27	Κατανομή προσωπικού, ανάπτυξη και διασφάλιση προσόντων αυτού	Το προσωπικό που απαιτείται για την επιτυχή σχεδίαση και υλοποίηση όλων των φάσεων και δομοστοιχείων του έργου έχει κατανεμηθεί σωστά, όσον αφορά πληθυσμό, ειδικότητες, εκπαίδευση και κονδύλια. Τα προσόντα του προσωπικού έχουν διασφαλιστεί με κατάλληλη επιλογή ή/και ανάπτυξη αυτών, χρονικά έγκαιρα και με ποιοτική επάρκεια.	Χρονοπρογραμματισμένη και διασφαλισμένης ποιότητας, αξιοπιστίας και αποδοχής διαδικασία επιλογής και κατανομής του προσωπικού που θα τοποθετηθεί στις διάφορες φάσεις του έργου. Προσμέτρηση ειδικών απαιτήσεων γλώσσας και πολιτισμικότητας. Διασφάλιση επαρκούς επιπέδου εκπαίδευσης/ειδίκευσης προσωπικού, μέσω ευρέως αποδεκτών διαδικασιών αξιολόγησης τυπικών και πραγματικών προσόντων και ανάπτυξής τους με την επιλογή κατάλληλων προγραμμάτων εκπαίδευσης/κατάρτισης.
28	Παρουσίαση, αιτιολόγηση και προώθηση του έργου στο προσωπικό κατώτερου κυβερνητικού/διοικητικού επιπέδου και το ευρύ κοινό (επίπεδο διοίκησης)	Το κατώτερο κυβερνητικό και διοικητικό προσωπικό, καθώς και το ευρύ κοινό είναι εξοικειωμένο με το έργο, θεωρεί ότι αιτιολογείται επαρκώς και πιστεύει στη χρησιμότητα, τους στόχους και τα αποτελέσματά του.	Εκστρατεία ενημέρωσης του κατώτερου διοικητικού και κυβερνητικού προσωπικού από τη διοίκηση του έργου, διαδικασίες αξιολόγησης των σταδίων του έργου από το προσωπικό, μέσω ερωτηματολογίων και online μηχανισμών αξιολόγησης, παροχή κινήτρων προς το προσωπικό για θετική κλίση προς το έργο, χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνη-

			σης.
29	Πρόβλεψη, διασφάλιση, παροχή και παρακολούθηση της αποτελεσματικότητας κινήτρων για την ορθή και υπεύθυνη υλοποίηση, λειτουργία και χρήση του έργου, από τους αναδόχους/εργολάβους, το προσωπικό υπηρεσίας και το κοινό στο οποίο απευθύνεται (επίπεδο διοίκησης)	Το προσωπικό υπηρεσίας, οι εργολάβοι/ανάδοχοι και το κοινό στο οποίο απευθύνεται το έργο, έχουν αποτελεσματικά κίνητρα για την ορθή και υπεύθυνη υλοποίηση, λειτουργία και χρήση του έργου και έχουν πίστη στους στόχους, τη λειτουργία και τα αποτελέσματά του.	Μελέτη και παροχή κατάλληλων κινήτρων (χρονικά, οικονομικά, κοινωνικά, ηθικά) για την ορθή και υπεύθυνη υλοποίηση, λειτουργία και χρήση του έργου. Τα κίνητρα θα πρέπει να καθοριστούν έγκαιρα και ανάλογα με τη φύση του έργου και το πώς αυτό υλοποιείται από τους αναδόχους/εργολάβους, πως εξυπηρετείται από το προσωπικό υπηρεσίας και πως επηρεάζει τη ζωή του κοινού στο οποίο απευθύνεται.
30	Ποιότητα διεπαφής διοίκησης, προσωπικού υπηρεσίας και τελικού χρήστη – σχεδίαση και διασφάλιση καλώς ορισμένων και αποτελεσματικών διαδικασιών, ευκολία πρόσβασης (επίπεδο διοίκησης)	Η διεπαφή μεταξύ διοίκησης, προσωπικού υπηρεσίας και τελικού χρήστη είναι καλώς ορισμένη, φιλική και εύκολα προσβάσιμη, έτσι ώστε να προωθεί την εύρυθμη λειτουργία του έργου, την επίτευξη των στόχων του και να επηρεάζει θετικά την γνώμη προς αυτό.	Προσεκτική, στοχοπροσανατολισμένη, λειτουργική και φιλική προς το προσωπικό και το χρήστη διεπαφή (επικοινωνία και διαδικασίες) μεταξύ της διοίκησης, του προσωπικού υπηρεσίας και του τελικού χρήστη. Η διεπαφή δίνει έμφαση στην επίτευξη των στόχων, με καλά ορισμένες και εύχρηστες διαδικασίες, ακόμα και οριακά σε βάρος της ασφάλειας.
31	Πίστη στα κίνητρα και στους τεθειμένους στόχους της πολιτικής ηγεσίας όσον αφορά το έργο (επίπεδο διοίκησης)	Η διοίκηση του έργου και του φορέα έχει πίστη στα πραγματικά κίνητρα και τους στόχους που έχουν οριστεί από την πολιτική ηγεσία, τόσο για το παρελθόν του περιβάλλοντος του έργου, όσο και για το μέλλον και τα αποτελέσματά του. Η διοίκηση πιστεύει ότι οι στόχοι που έχουν τεθεί και τα αναμενόμενα αποτελέσματα θα είναι προς όφελος της ίδιας και του οργανισμού που διοικεί και αποτελεί φορέα σχετιζόμενο με τις φάσεις ή τα αποτελέσματα του έργου.	Η πολιτική ηγεσία έχει επιδείξει σταθερή προσήλωση στους στόχους, στην ολοκλήρωση και στα αποτελέσματα του έργου, έχει ιστορικά πείσει σε παρόμοια ή συμπληρωματικά έργα για τα παραπάνω, προς τελικό όφελος της διοίκησης και των οργανισμών φορέων και τελικά του ευρύτερου κοινού στο οποίο απευθύνεται το έργο. Ενημέρωση της πολιτικής ηγεσίας για την πολιτική που πρέπει να επιδείξει και τις ενέργειας που πρέπει να ακολουθήσει, προς όφελος του έργου, των σκοπών του και της θετικής άποψης του προσωπικού και του κοινού προς αυτό.
Γ	***Επίπεδο προσωπικού υπηρεσίας***		
32	Εξοικείωση και εκπαίδευση του κατανεμηθέντος προσωπικού	Το προσωπικό υπηρεσίας που έχει οριστεί για το έργο είναι επαρκώς εξοικειωμένο και εκπαιδευμένο για να α-	Διαδικασίες, εκστρατείες και προγράμματα ενημέρωσης και εκπαίδευσης του προσωπικού. Παροχή κινήτρων για

		νταποκριθεί σε τακτικές και έκτακτες λειτουργικές και υποστηρικτικές ανάγκες του έργου, σε όλες τις φάσεις του. Το προσωπικό διαθέτει κίνητρα που διασφαλίζουν το ενδιαφέρον, τη διάδραση και την υπευθυνότητά του προς το έργο και την ανταπόκριση στις απαιτήσεις του.	να κινηθεί το ενδιαφέρον και να διασφαλιστεί επαρκής εκπαίδευση, κατάρτιση και υπευθυνότητα του προσωπικού.
33	Φιλικότητα του συστήματος προς το προσωπικό υπηρεσίας	Το σύστημα διαθέτει κατανοητή, λειτουργική και ευνόητη διεπαφή με το προσωπικό υπηρεσίας, το οποίο μπορεί να επιτελεί την εργασία του με βατό και ευχάριστο τρόπο και περιβάλλον, προς όφελος της λειτουργίας και της υποστήριξης του έργου. Το προσωπικό υπηρεσίας διαθέτει εύκολη πρόσβαση σε υλικό καθοδήγησης και αναφοράς, όπου και όταν χρειάζεται βοήθεια για να ανταποκριθεί σε απαιτήσεις του συστήματος. Το τελευταίο περιλαμβάνει και διεπαφή με τεχνικό προσωπικό του ανάδοχου/εργολάβου.	Χρησηστραφής σχεδίαση και υλοποίηση του συστήματος με ισορροπία ανάμεσα στις απαιτήσεις λειτουργικότητας και στους περιορισμούς ασφάλειας. Σχεδιασμός και υλοποίηση επιγραμμικής βοήθειας στη διαχείριση του συστήματος και αποτελεσματικών διαδικασιών επικοινωνίας και υπηρεσιών υποστήριξης από τον ανάδοχο/εργολάβο προς το προσωπικό ασφάλειας. Οι παράγοντες αυτοί πρέπει να ξεκινήσουν από τη φάση της σύνταξης των προδιαγραφών του συστήματος, πολύ πριν την υλοποίηση και λειτουργία του συστήματος και να συνεχιστούν με διαδικασίες αυτοαξιολόγησης και διόρθωσης σε όλες τις επόμενες φάσεις του, μέχρι και την παραγωγική λειτουργία. Επειδή το αίσθημα φιλικότητας του συστήματος είναι πολλές φορές υποκειμενικό, υλοποίηση σεμινάριων και εκστρατειών ενημέρωσης, τα οποία να διαθέτουν σημαντικό στοιχείο πειθούς του προσωπικού υπηρεσίας, καθώς και παροχή κινήτρων για την διαμόρφωσης ευνοϊκής άποψης για το σύστημα.
34	Αρμόζον τεχνικό επίπεδο (μπορεί να επηρεάσει σε μεγάλο βαθμό την απόδοση του προσωπικού υπηρεσίας σε απρόβλεπτες καταστάσεις)	Το προσωπικό υπηρεσίας έχει την τεχνική εκπαίδευση και κατάρτιση σε επαρκές βαθμό για να ανταποκριθεί αυτόνομα σε οιεσδήποτε τακτικές ή έκτακτες απαιτήσεις του συστήματος και των χρηστών του, κάτω από οποιεσδήποτε συνθήκες, χωρίς να χρειάζεται η συνδρομή του ανάδοχου/εργολάβου. Εναλλακτικά υπάρχει επαρκές	Σχεδίαση και υλοποίηση ολοκληρωμένου περιβάλλοντος προώθησης τεχνικής κουλτούρας, επιλογής κατάλληλου προσωπικού, τεχνικής εκπαίδευσης και κατάρτισης, αξιολόγησης και ελέγχου επιπέδου γνώσεων, παροχής κινήτρων βελτίωσης και απόδοσης. Οι παράγοντες αυτοί πρέπει να είναι αυστηρά στοχοστραφείς και υπηρεσιοστρα-

		συμβόλαιο υποστήριξης (SLA) για την εξυπηρέτηση των αναγκών αυτών από τον ανάδοχο/εργολάβο. Τελικός στόχος, οι χρήστες του συστήματος να αισθάνονται ότι έχουν δίπλα τους υποστήριξη που μπορεί να τους βοηθήσει σε οποιοδήποτε πρόβλημά τους.	φείς, προς τη διασφάλιση των αναγκών της υπηρεσίας του συστήματος.
35	Κίνητρα για την σωστή, ασφαλή και αποτελεσματική χρήση του συστήματος	Το προσωπικό υπηρεσίας διαθέτει πραγματικά κίνητρα (όχι μόνο κανόνες και υποχρεώσεις), για την ορθή, ασφαλή και αποτελεσματική χρήση του συστήματος. Τα κίνητρα ωθούν προς όφελος του συστήματος και δεν προσπίπτουν σε εμπόδια δικαιοδοσίας, κανονιστικών, νομικών, λειτουργικών ή περιορισμών ασφάλειας, ή αντικίνητρα οποιουδήποτε είδους.	Εξ' αρχής πρόβλεψη, σχεδίαση και διασφάλιση κατάλληλων κινήτρων, ανάλογων με τις προσδοκίες του προσωπικού. Διασφάλιση αντικειμενικής παροχής αυτών, προς όφελος του συστήματος και της ασφαλούς και αποτελεσματικής χρήσης του και όχι προς όφελος συγκεκριμένων ομάδων, συμφερόντων ή αλλότριων στόχων. Πρόβλεψη, σχεδιασμός και διασφάλιση αφαίρεσης εμποδίων που αντίκεινται στα κίνητρα αυτά, όπως και πιθανών αντικινήτρων.
36	Κίνητρα για την ταχεία, αποτελεσματική και ευγενή υποστήριξη των τελικών χρηστών	Τα κίνητρα που παρέχονται στο προσωπικό υπηρεσίας ωθούν προς τη βελτίωση της ψυχολογικής του κατάστασης προς όφελος του συστήματος και δεν αποτελούν καταναγκαστικά μέτρα που τους δεσμεύουν σε ψεύτικη διάθεση, η οποία αργά ή γρήγορα γίνεται αντιληπτή από τους χρήστες. Οι τελικοί χρήστες νιώθουν πως εξυπηρετούνται εγκαίρως, επαρκώς, αποτελεσματικά και χωρίς πολύπλοκες, χρονοβόρες και δυσνόητες διαδικασίες, είναι δε ευχαριστημένοι από τους τρόπους και την διάθεση του προσωπικού υπηρεσίας.	Εξ' αρχής πρόβλεψη, σχεδίαση και διασφάλιση κατάλληλων κινήτρων, ανάλογων με τις προσδοκίες του προσωπικού. Διασφάλιση αντικειμενικής παροχής αυτών, προς όφελος του συστήματος και της αποτελεσματικής και ικανοποιητικής υποστήριξης των χρηστών και όχι προς όφελος συγκεκριμένων ομάδων, συμφερόντων ή αλλότριων στόχων. Πρόβλεψη, σχεδιασμός και διασφάλιση αφαίρεσης εμποδίων που αντίκεινται στα κίνητρα αυτά, όπως και πιθανών αντικινήτρων. Διασφάλιση ότι τα κίνητρα που παρέχονται στο προσωπικό υπηρεσίας ωθούν προς τη βελτίωση της ψυχολογικής του κατάστασης προς όφελος του συστήματος και δεν αποτελούν καταναγκαστικά μέτρα που τους δεσμεύουν σε ψεύτικη διάθεση, η οποία αργά ή γρήγορα γίνεται αντιληπτή από τους χρήστες.
37	Ανατροπή εξουσιών, αρμοδιοτήτων και	Το έργο, οι υπηρεσίες, οι αρμοδιότητες, οι τεχνολογίες και	Ειδική ανάλυση και σχεδιασμός για την αντιμετώπιση

	ισορροπιών λόγω νέων τεχνολογιών και γνώσης – δημιουργία φραγμών, κλειστών ομάδων και ανταγωνισμού (επίπεδο προσωπικού υπηρεσίας)	η προβολή που εισάγει/προκαλεί στους φορείς που μετέχουν (στο επίπεδο του προσωπικού υπηρεσίας) δεν προκαλεί ανατροπή εξουσιών, αρμοδιοτήτων και ισορροπιών, φραγμούς, κλειστές ή προνομιούχες ομάδες και επιζήμιο ανταγωνισμό. Αντίθετα, λειτουργεί ως μέσο προώθησης κοινού συμφέροντος, ωφελημάτων, τεχνολογικής αναβάθμισης, συνεργασίας, ομοψυχίας και αρμονικής συνύπαρξης.	θεμάτων εξουσιών, αρμοδιοτήτων και ισορροπιών, στις φάσεις προκήρυξης και υλοποίησης του έργου. Δημιουργία ομάδας εργασίας στο επίπεδο της διοίκησης για την εποπτεία και την αντιμετώπιση προβλημάτων αυτού του είδους. Δημιουργία καναλιού επικοινωνίας με την πολιτική ηγεσία για την αντιμετώπιση τέτοιων προβλημάτων, σε όλες τις φάσεις του έργου. Έμφαση στην πρόληψη, αντί της εκ των υστέρων αντιμετώπισης.
38	Αλλαγή καθηκόντων που μπορεί να απαιτηθούν από οργανωτικές και διαδικαστικές μεταβολές, είτε για την υποστήριξη, είτε ως αποτέλεσμα της υλοποίησης του έργου	Οργανωτικές και διαδικαστικές μεταβολές, καθώς και τυχόν αλλαγές καθηκόντων προσωπικού που απαιτούνται από αυτές, είτε για την υποστήριξη, είτε ως αποτέλεσμα της υλοποίησης του έργου/συστήματος, γίνονται σχεδιασμένα και προμελετημένα, λαμβάνοντας υπόψη τις επιπτώσεις τους, έτσι ώστε να μην αποτελούν τροχοπέδη για την υλοποίηση ή τη λειτουργία του έργου/συστήματος. Λαμβάνονται υπόψη παράγοντες όπως η κατάρτιση και οι επιθυμίες του προσωπικού, τα κίνητρα που απαιτούνται και τα πραγματικά αποτελέσματα του έργου, όχι απλά οι επιθυμητοί στόχοι.	Σχεδιασμός οργανωτικών, εργασιακών και διαδικαστικών μεταβολών και αντιστοίχων αλλαγών σε καθήκοντα του προσωπικού υπηρεσίας, σε όλες τις φάσεις του έργου, έτσι ώστε αυτές να γίνονται προμελετημένα, με το μικρότερο αντίκτυπο και όχι ως εκ των υστέρων αντίδραση σε προβλήματα ή ανεπάρκειες. Σχεδιασμός και υλοποίηση διαδικασιών ταχείας αντίδρασης σε προβλήματα και ανάγκες που δεν έχουν προβλεφθεί. Παροχή κινήτρων, όπου απαιτούνται, για την επιτυχία των αλλαγών. Υπολογισμός παραγόντων όπως η κατάρτιση, η εμπειρία και οι επιθυμίες του προσωπικού, τα κίνητρα που απαιτούνται και τα πραγματικά αποτελέσματα του έργου, όχι απλά οι επιθυμητοί στόχοι.
39	Φόβοι απώλειας εργασίας με την υιοθέτηση νέων τεχνολογικών και διαδικασιών	Δεν επιδρούν ανασταλτικοί παράγοντες όπως ο φόβος απώλειας εργασίας, ή υποβάθμισής της, ως αποτέλεσμα της υλοποίησης ή της λειτουργίας του έργου. Η τεχνολογία και οι διαδικασίες που αυτό εισάγει προωθούν ή μεταλλάσουν την εργασία του προσωπικού των φορέων υλοποίησης, όπου αυτό είναι δυνατό. Διαφορετικά, συγκροτημένη μετάταξη του προσωπικού σε άλλους τομείς/καθήκοντα/υπευθυνότητες, χωρίς απαξίωσή τους ή	Ειδική μελέτη, σχεδιασμός και δράση έτσι ώστε να μην επιδρούν ανασταλτικοί παράγοντες όπως ο φόβος απώλειας εργασίας, ή υποβάθμισής της, ως αποτέλεσμα της υλοποίησης ή της λειτουργίας του έργου. Πρόβλεψη για προώθηση ή μεταλλαγή της εργασίας και της κατάρτισης του προσωπικού, όπου αυτό είναι δυνατό, με επιμορφωτικά προγράμματα και κίνητρα εξέλιξης. Διαφορετικά ,συγκροτημένη μετάταξη του προσωπικού σε άλλους το-

		πρόκληση παθητικής ή ενεργητικής αντίδρασης που μπορεί να αποτελέσει ανασταλτικό παράγοντα για την επιτυχία.	μείς/καθήκοντα/υπευθυνότητες, χωρίς απαξίωση ή πρόκληση αντιδράσεων που μπορεί να αποτελέσουν ανασταλτικό παράγοντα για την επιτυχία του έργου. Παροχή κινήτρων προς το προσωπικό και μελέτη των αρμοδιοτήτων/τμημάτων/φορέων που έχουν ανάγκη για το πλεονάζων προσωπικό. Ενημέρωση του προσωπικού σε κάθε στάδιο και εποικοδομητική συμμετοχή του στις διαδικασίες.
40	Ικανότητες επικοινωνίας του προσωπικού υπηρεσίας – επηρεάζει σημαντικά την αποτελεσματικότητά του (επίπεδο προσωπικού υπηρεσίας)	Το προσωπικό υπηρεσίας έχει την κατάλληλη εκπαίδευση και ικανότητες επικοινωνίας με τους τελικούς χρήστες που υποστηρίζει ώστε να είναι αποτελεσματικό, με τελικό στόχο την ικανοποίησή τους. Το προσωπικό έχει τα κίνητρα για τη διασφάλιση της ποιότητα επικοινωνίας, μαζί με καλώς ορισμένους κανόνες ανταπόκρισης, συμπεριφοράς και δεοντολογίας.	Εκπαίδευση του προσωπικού προς ανάπτυξη των ικανοτήτων επικοινωνίας, παράλληλα με την τεχνική κατάρτιση. Παροχή κινήτρων που θα διασφαλίζουν την ποιότητα της επικοινωνίας και σύνδεσή τους με διαδικασίες αντικειμενικής αξιολόγησής της. Μορφοποίηση καλώς ορισμένων κανόνων ανταπόκρισης, συμπεριφοράς και δεοντολογίας, καθώς και διαδικασιών διασφάλισής των. Συμμετοχή του προσωπικού υπηρεσίας στη σύνταξη των κανόνων, καθώς σε άλλες παρεμφερείς υπηρεσίες υποστήριξης.
41	Ποιότητα διεπαφής προσωπικού υπηρεσίας / τελικού χρήστη – υιοθέτηση καλώς ορισμένων και αποτελεσματικών διαδικασιών, ευκολία πρόσβασης (επίπεδο προσωπικού υπηρεσίας)	Το προσωπικό υπηρεσίας έχει την κατάλληλη εκπαίδευση και ικανότητες επικοινωνίας με τους τελικούς χρήστες που υποστηρίζει ώστε να είναι αποτελεσματικό, με τελικό στόχο την ικανοποίησή τους. Το προσωπικό έχει τα κίνητρα για την ποιότητα της επικοινωνίας, μαζί με καλώς ορισμένους κανόνες συμπεριφοράς και δεοντολογίας. Η διεπαφή με τον τελικό χρήστη διαθέτει καλώς ορισμένες διαδικασίες, κανόνες και μέτρα διασφάλισης της ποιότητας. Υπάρχει εύκολη πρόσβαση στην υπηρεσία υπό οιεσδήποτε συνθήκες, με τρόπους που μπορούν να χρησιμοποιήσουν όλες οι κατηγορίες των χρηστών και επαρ-	Εκπαίδευση του προσωπικού προς ανάπτυξη των ικανοτήτων επικοινωνίας και της τεχνικής κατάρτισης. Παροχή κινήτρων που θα διασφαλίζουν την ποιότητα της επικοινωνίας και σύνδεσή τους με διαδικασίες αντικειμενικής αξιολόγησής της. Καλώς ορισμένοι κανόνες συμπεριφοράς και δεοντολογίας και διαδικασίες διασφάλισής τους. Υλοποίηση καλώς ορισμένων διαδικασιών, κανόνων και μέτρων διασφάλισης της ποιότητας της επικοινωνίας. Παροχή πολλαπλών τρόπων πρόσβασης στην υπηρεσία, εύκολα προσβάσιμων από τους τελικούς χρήστες, με ελαχιστοποίηση του κόστους και επαρκή γεωγραφική κάλυ-

		κή γεωγραφική κάλυψη.	ψη. Χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.
42	Πίστη στα κίνητρα και στους τεθειμένους στόχους του συστήματος από την πολιτική ηγεσία και την διοίκηση (επίπεδο προσωπικού υπηρεσίας)	Το προσωπικό υπηρεσίας έχει πίστη και εμπιστοσύνη στα κίνητρα και τους στόχους που έχουν τεθεί από την πολιτική ηγεσία και την διοίκηση του έργου, τόσο για το παρελθόν του περιβάλλοντός του, όσο και για το μέλλον και τα αποτελέσματα του ίδιου του έργου. Το προσωπικό πιστεύει ότι οι στόχοι που έχουν τεθεί και τα αναμενόμενα αποτελέσματά του είναι ρεαλιστικά και προς όφελος των ιδίων και των οργανισμών που σχετίζονται με τις φάσεις ή τα αποτελέσματα του έργου.	Η πολιτική ηγεσία έχει επιδείξει σταθερή προσήλωση στους στόχους, στην ολοκλήρωση και στα αποτελέσματα του έργου και έχει ιστορικά πείσει σε παρόμοια ή συμπληρωματικά έργα για τα παραπάνω, προς τελικό όφελος της διοίκησης, του προσωπικού, των οργανισμών φορέων και τελικά του ευρύτερου κοινού στο οποίο απευθύνεται το έργο. Ενημέρωση της διοίκησης και του προσωπικού για την πολιτική που πρέπει να επιδείξει και τις ενέργειας που πρέπει να ακολουθήσει, προς όφελος του έργου, των σκοπών του και της θετικής άποψης του κοινού προς αυτό.
Δ	***Επίπεδο Αναδόχου/Εργολάβου***		
43	Δεξιότητες και τεχνική κατάρτιση προσωπικού	Το προσωπικό του αναδόχου/εργολάβου έχει τις δεξιότητες, την τεχνική κατάρτιση και την εμπειρία για να ανταποκριθεί στις τακτικές και έκτακτες απαιτήσεις του έργου.	Αντικειμενική και σύμφωνα με τις απαιτήσεις του έργου επιλογή αναδόχου (όπου αυτό είναι δυνατό), ή/και σύνταξη του διαγωνισμού του έργου ώστε να διασφαλίζεται η επιλογή του κατάλληλου αναδόχου, ο οποίος θα διαθέτει την κατάρτιση και εμπειρία για να ανταποκριθεί στις τακτικές και έκτακτες απαιτήσεις του έργου. Διασφάλιση των πραγματικών ικανοτήτων του προσωπικού, καθώς και των διαδικασιών του αναδόχου/εργολάβου μέσω διεθνών πιστοποιήσεων ποιότητας διαδικασιών, τεχνικής κατάρτισης και ασφάλειας. Προσωπικές συνεντεύξεις με το προσωπικό του αναδόχου/εργολάβου. Επιλογή κατάλληλου προσωπικού του φορέα του έργου που θα διενεργήσει τη σύνταξη των προδιαγραφών, την επιλογή και την αξιολόγηση του αναδόχου/εργολάβου.
44	Τεχνολογική αρτιότητα και μακροχρόνια	Ο ανάδοχος/εργολάβος διαθέτει ολική τεχνολογική αρτιό-	Αντικειμενική και σύμφωνα με τις απαιτήσεις του έργου

	επένδυση σε αυτή	τητα, ως τεχνογνωσία οργανισμού και όχι ως κατάρτιση επιμέρους στελεχών του. Επενδύει μακροχρόνια σε αυτήν, μέσω εκπαιδεύσεων και κινήτρων προς το προσωπικό του και επιδιώκει αντίστοιχα έργα. Διαθέτει τις διαδικασίες για την υποστήριξη αυτής της προσπάθειας, οι οποίες περιλαμβάνουν αλληλεπικαλυπτόμενο προσωπικό και τεχνογνωσία, χωρίς να υπάρχει εξάρτηση από ένα άτομο ή τομέα.	επιλογή αναδόχου (όπου αυτό είναι δυνατό), ή/και σύνταξη του διαγωνισμού του έργου ώστε να διασφαλίζονται: α) η επιλογή κατάλληλου αναδόχου, ο οποίος θα έχει επιδείξει τεχνολογική αρτιότητα και μακροχρόνια επένδυση σε αυτή, β) οι πραγματικές ικανότητες του προσωπικού και η ποιότητα διαδικασιών του αναδόχου/εργολάβου μέσω διεθνών πιστοποιήσεων ποιότητας διαδικασιών, τεχνικής κατάρτισης και ασφάλειας, γ) η ύπαρξη αλληλεπικαλυπτόμενου προσωπικού και τεχνογνωσίας, χωρίς εξάρτηση από ένα άτομο ή τομέα. Προσωπικές συνεντεύξεις με το προσωπικό του αναδόχου/εργολάβου. Επιλογή του κατάλληλου προσωπικού του φορέα του έργου που θα διενεργήσει τη σύνταξη των προδιαγραφών, την επιλογή και την αξιολόγηση του αναδόχου/εργολάβου.
45	Παρελθούσα εμπειρία σχετική με το έργο	Ο ανάδοχος/εργολάβος διαθέτει εμπειρία από αντίστοιχα, παρόμοια, παράλληλα ή συμπληρωματικά έργα σε άλλους φορείς, ή ακόμα πιο σημαντικά, στον ίδιο φορέα με αυτόν που υλοποιεί το έργο. Τα έργα αυτά έχουν ολοκληρωθεί επιτυχώς και έχουν πετύχει τους στόχους τους. Ο ανάδοχος/εργολάβος έχει ίδια μέσα, εμπειρία και τεχνογνωσία στην υλοποίηση των έργων και την έχει διατηρήσει. Ο φορέας υλοποίησης έχει θετική εμπειρία και συνεργασία από παρελθόντα έργα του αναδόχου/εργολάβου.	Αντικειμενική και σύμφωνα με τις απαιτήσεις του έργου επιλογή αναδόχου (όπου αυτό είναι δυνατό), ή/και σύνταξη του διαγωνισμού του έργου ώστε να διασφαλίζεται η επιλογή κατάλληλου αναδόχου, ο οποίος θα έχει παρελθούσα εμπειρία σε παρόμοια έργα, στον ίδιο ή σε άλλους οργανισμούς, τα οποία θα έχουν ολοκληρωθεί και επιτύχει στους στόχους τους. Επιλογή του κατάλληλου προσωπικού του φορέα του έργου που θα διενεργήσει τη σύνταξη των προδιαγραφών, την επιλογή και την αξιολόγηση του αναδόχου/εργολάβου.
46	Παρελθούσα εμπειρία με τον φορέα του έργου	Ο ανάδοχος/εργολάβος διαθέτει εμπειρία με έργα ή τεχνική υποστήριξη με τον φορέα/φορείς του έργου, γνωρίζοντας ως αποτέλεσμα προσωπικό, συστήματα, διαδικασίες και συνθήκες και αυτό αποτελεί βοήθεια στην υλοποίηση και την επίτευξη των στόχων του. Το προσωπικό του	Επιλογή αναδόχου/εργολάβου ανάλογα και με την παρελθούσα εμπειρία του με τον φορέα/φορείς του έργου. Σύνταξη του διαγωνισμού του έργου έτσι ώστε να πριμοδοτεί αναδόχους που έχουν πρότερη εμπειρία με τον φορέα/φορείς του έργου.

		φορέα είναι εξοικειωμένο με τον ανάδοχο/εργολάβο και αυτό διευκολύνει την επικοινωνία και τη συνεργασία με το προσωπικό του.	
47	Δεξιότητες επικοινωνίας (προφορική και γραπτή)	Το προσωπικό του αναδόχου διαθέτει επαρκείς δεξιότητες, μαζί με οργάνωση για την προφορική επικοινωνία, τη σύνταξη αναφορών, τεκμηριώσεων και άλλων κειμένων σχετικών με το έργο. Οι δεξιότητες αυτές εφαρμόζονται αποτελεσματικά στην επικοινωνία προς τη διοίκηση, την πολιτική ηγεσία και το προσωπικό του φορέα/φορέων του έργου.	Επιλογή αναδόχου/εργολάβου ανάλογα με την παρελθούσα επίδοσή του (επικοινωνιακά) σε άλλα έργα. Σύνταξη του διαγωνισμού έτσι ώστε να πριμοδοτεί αναδόχους, ανάλογα με την απόδοσή τους σε παρελθόντα ανάλογα ή παρόμοια έργα του ιδίου ή άλλων φορέων. Δημιουργία των κατάλληλων οργανωτικών δομών, διαδικασιών και κανονισμών που να προάγουν την επικοινωνία και την τεκμηρίωση, με αντικειμενική αξιολόγηση της επίδοσης του φορέα και του ανάδοχου και λήψη διορθωτικών μέτρων, όπου απαιτείται. Χρήση τεχνολογιών ηλεκτρονικής τεκμηρίωσης, συνεργασίας και διοίκησης.
48	Κίνητρα/δεσμεύσεις για σωστή υλοποίηση και υποστήριξη του έργου	Ο ανάδοχος/εργολάβος είναι δεσμευμένος τυπικά για την ορθή εκτέλεση του έργου, σύμφωνα με τα χαρακτηριστικά, την προσφορά και τη σύμβαση εκτέλεσης . Επίσης, αποδέχεται και συμμερίζεται τους στόχους του έργου, την ορθότητα, την ερμηνεία τους και τον τρόπο αξιολόγησής τους. Εκτός αυτών έχει και πραγματικά κίνητρα για τα παραπάνω, έτσι ώστε να μην προσπαθεί να παρερμηνεύσει τις δεσμεύσεις του, τους στόχους του έργου και τα κριτήρια αξιολόγησής του.	Σύνταξη συμβάσεων και λοιπού κανονιστικού πλαισίου συμβατικών υποχρεώσεων του αναδόχου με τρόπο που να διασφαλίζει ορθή εκτέλεση του έργου, τήρηση των προδιαγραφών, επίτευξη των στόχων, αντικειμενική αξιολόγηση και αδυναμία αποκήρυξης ευθύνης. Δημιουργία των κατάλληλων δομών από τη πλευρά του φορέα του έργου για την παρακολούθηση της ορθής εκτέλεσης και των ενεργειών του αναδόχου. Πρόβλεψη και παροχή προς τον ανάδοχο όσο το δυνατό ικανών κινήτρων, έτσι ώστε να μην ωθείται μόνο από συμβατικές υποχρεώσεις, αλλά και από ίδιο συμφέρον και θέληση. Σύνταξη ορθής μελέτης υλοποίησης, η οποία περιλαμβάνει μετρικά και διαδικασίες αντικειμενικής αξιολόγησης του έργου, του αναδόχου και των αποτελεσμάτων της εκτέλεσης.
49	Ακριβής υλοποίηση της επιχειρηματικής	Ο ανάδοχος/εργολάβος υλοποιεί με ακρίβεια το έργο,	Δημιουργία δομών παρακολούθησης και παραλαβής του

	περίπτωσης, σχεδίασης και χαρακτηριστικών	σύμφωνα με τις συμβατικές του υποχρεώσεις, προς την επίτευξη των στόχων του. Η επιχειρηματική περίπτωση, η σχεδίαση και τα χαρακτηριστικά του έργου που έχουν απεικονιστεί σε αυτά είναι ορθά και αντανακλούν τους στόχους του έργου. Υπάρχει αντικειμενική παρακολούθηση και αξιολόγηση της πορείας του έργου και των στόχων του από τον φορέα του έργου, τον ανάδοχο και ιδεατά από τρίτους ανεξάρτητους ελεγκτικούς φορείς.	έργου, με διαδικασίες αντικειμενικής αξιολόγησης ικανοτήτων, εμπειρίας και τεχνικής κατάρτισης. Ανάθεση σε αυτές μη μετακλητής δικαιοδοσίας για την αξιολόγηση και την παραλαβή του έργου. Δημιουργία και λειτουργία λεπτομερών διαδικασιών παρακολούθησης, ελέγχου, αξιολόγησης και επικοινωνίας. Δημιουργία ευέλικτων διαδικασιών επαναπροσδιορισμού ενεργειών και στόχων για την αντιμετώπιση απρόβλεπτων καταστάσεων. Αποσύνδεση της εξουσίας της παρακολούθησης και παραλαβής από την εξουσία, τα συμφέροντα και τις προσωπικές επιθυμίες της διοίκησης και της πολιτικής ηγεσίας, προς όφελος του έργου.
50	Ακριβής και πλήρης τεκμηρίωση διαδικασιών, λεπτομερειών υλοποίησης και παραλλαγοδότησης (versioning)	Ο ανάδοχος υλοποιεί αναλυτική και ακριβή τεκμηρίωση των διαδικασιών του, των λεπτομερειών της υλοποίησης του έργου, καθώς και σύστημα παραλλαγοδότησης, όπου εφαρμόζεται. Το υλικό αυτό είναι δομημένο και ανοικτό, έτσι ώστε να είναι κατανοητό από το προσωπικό και τη διοίκηση του φορέα του έργου, καθώς και από το ευρύτερο κοινό, όπου απαιτείται. Ο φορέας αποκτά σαν αποτέλεσμα πλήρη γνώση του έργου/συστήματος, έτσι ώστε να μπορεί να ανταποκριθεί σε μελλοντικές απαιτήσεις ή αξιολογήσεις αυτού ή άλλων παρόμοιων έργων.	Ορισμός υποχρεώσεων ακριβούς και πλήρους τεκμηρίωσης διαδικασιών και λεπτομερειών υλοποίησης και παραλλαγοδότησης, σαν μέρος των συμβατικών υποχρεώσεων του ανάδοχου, στα χαρακτηριστικά, τη μελέτη υλοποίησης και τις διαδικασίες αξιολόγησης του έργου. Παρακολούθηση και αξιολόγηση αυτών από την ομάδα παρακολούθησης και παραλαβής. Πρόβλεψη και παροχή κινήτρων προς τον ανάδοχο προς αυτό το σκοπό.
51	Θετικές προς την έκβαση του έργου σχέσεις με την πολιτική και διοικητική ιεραρχία	Ο ανάδοχος/εργολάβος έχει θετικές για την έκβαση του έργου, την ολοκλήρωσή του και την επίτευξη των στόχων του σχέσεις με την πολιτική και διοικητική ιεραρχία. Αυτές λειτουργούν έτσι ώστε να μπορούν να κάμψουν δυσκολίες, εμπόδια και αλλότρια συμφέροντα, όπου υπάρχουν και δεν έχουν προβλεφθεί έτσι ώστε να έχουν ληφθεί μέτρα, προς όφελος του έργου και του φορέα υλοποίησης	Καλλιέργεια θετικών προς την ολοκλήρωση και τους στόχους του έργου σχέσεων, επικοινωνίας και διαδικασιών του ανάδοχου με την πολιτική ηγεσία και διοίκηση των εμπλεκομένων φορέων. Οι σχέσεις αυτές πρέπει να περιλαμβάνουν και το προσωπικό των φορέων που εμπλέκεται στην υλοποίηση και τη λειτουργία του έργου, έτσι ώστε να μην αποτελούν τροχοπέδη και παράγοντα αποδό-

		και όχι προς όφελος του αναδόχου ή τρίτων.	μησης των σχέσεων.
52	Πιστοποίηση οργάνωσης, διαδικασιών, τεχνικής κατάρτισης και ασφάλειας, σύμφωνα με διεθνή πρότυπα και ελεγκτικούς μηχανισμούς	Η οργάνωση, οι διαδικασίες και η τεχνική κατάρτιση, όπως και η ασφάλεια αυτών και των συστημάτων (υλικά, πρωτόκολλα, διεργασίες) είναι σύμφωνη με διεθνή πρότυπα και υπόκεινται στον έλεγχο ειδικευμένων εγχώριων ή διεθνών ελεγκτικών οργανισμών.	Ορισμός πιστοποιήσεων οργάνωσης, διαδικασιών, τεχνικής κατάρτισης και ασφάλειας στα χαρακτηριστικά, τις συμβάσεις και τη μελέτη υλοποίησης του έργου. Εξοικείωση του προσωπικού σύνταξης χαρακτηριστικών, διαγωνισμού, συμβάσεων και παρακολούθησης και παραλαβής του έργου με αυτά και αντίστοιχος έλεγχος του ανάδοχου. Ορισμός ελεγκτικών μηχανισμών ή/και οργανισμών για την παρακολούθηση, εφαρμογή και πιστοποίηση αυτών.
Ε	***Επίπεδο τελικού χρήστη/***		
53	Εξοικείωση με το έργο	Βασική γνώση των τελικών χρηστών για το αντικείμενο του έργου και το πως αυτό θα βελτιώσει τη ζωή τους και την αλληλεπίδρασή τους με την κυβέρνηση και τη δημόσια διοίκηση.	Εκστρατεία γνωριμίας και προώθησης του έργου, διαφημίσεις, διανομή φυλλαδίων, λευκά έγγραφα (white papers), χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.
54	Τεχνολογική κουλτούρα	Οι τελικοί χρήστες διαθέτουν βασική κατανόηση της σχετικής με το έργο τεχνολογίας, των διαδικασιών που ενέχει και των ωφελημάτων που προσφέρει.	Εύκολα προσβάσιμοι και ευκολο-κατανόητοι οδηγοί χρήσης, μέθοδοι τεχνολογικής διείσδυσης (πχ. συνεργασία με ISPs, σχολεία, εκθέσεις, μουσεία, τοπικές αρχές), χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.
55	Φιλικότητα χρήσης του συστήματος	Οι τελικοί χρήστες κατανοούν βασική πλοήγηση και διαδικασίες στο σύστημα, χωρίς την ανάγνωση υπερβολικής ποσότητας εγχειριδίων.	Εύκολο στην κατανόηση γραφικό περιβάλλον χρήσης με βοήθεια βάσει συγκειμένου (context sensitive help). Σχεδίαση της διαπροσωπείας του συστήματος βάσει απόψεων και δεξιοτήτων χρηστών ή αντιπροσωπευτικών ομάδων, καθώς και διεθνών προτύπων και βέλτιστων πρακτικών.
56	Εμπιστοσύνη προς το σύστημα, ιδιαίτερα όπου υπάρχει θέμα αποθήκευσης και χρήσης προσωπικών/ιδιωτικών δεδομέ-	Οι τελικοί χρήστες εμπιστεύονται τα προσωπικά τους δεδομένα και συναλλαγές στο σύστημα και στην αρχή που το διαχειρίζεται ή/και χειρίζεται.	Πιστοποίηση του συστήματος και των διαδικασιών που εφαρμόζει από αρχή προστασίας δεδομένων προσωπικού χαρακτήρα ή/και φορείς ελέγχου και πιστοποίησης

	νων		ασφάλειας, χρήση μηχανισμών ανθεκτικών στην παραποίηση, χρήση υλικών με διεθνείς πιστοποιήσεις ασφάλειας, χρήση τρίτων οργανισμών ή αναδόχων με πιστοποίηση ποιότητας διαδικασιών ή ασφάλειας, ενημέρωση των χρηστών για τα χαρακτηριστικά ασφάλειας εντός των μεθόδων εξοικείωσης με το σύστημα, κανονιστικό και νομικό πλαίσιο που να προάγει την ασφάλεια και την αποτρέπει την αποκήρυξης ευθύνης.
57	Κίνητρα για χρήση (οικονομικά, χρονικά, ανάγκες)	Οι τελικοί χρήστες χρησιμοποιούν το σύστημα γιατί τους συμφέρει οικονομικά και χρονικά, σε σχέση με τη φυσική τους παρουσία (ή τη χρήση μέσω τρίτων) και τους παρέχονται περισσότερες δυνατότητες. Το έργο ανταποκρίνεται σε πραγματικές ανάγκες και επιθυμίες, ακόμα και αν αυτές είναι τεχνητές.	Εύκολη πρόσβαση σε ηλεκτρονικές υπηρεσίες που μειώνουν την ανάγκη για φυσική παρουσία, μικρότερες διαχειριστικές απαιτήσεις, πρόσβαση σε προωθημένες υπηρεσίες αν χρησιμοποιηθεί το σύστημα (πχ. έξυπνες κάρτες και υποδομή ΥΔΚ). Μελέτη σκοπιμότητας και επιχειρηματική τοποθέτηση του έργου ώστε να ανταποκρίνεται σε πραγματικές ανάγκες των ενδιαφερόμενων φορέων, ομάδων, χρηστών. Εκστρατεία δημιουργίας κινήτρων και αναγκών στους χρήστες (εφόσον οι πραγματικές δεν επαρκούν/υπάρχουν) μέσω των ΜΜΕ.
58	Κίνητρα για υπεύθυνη/ασφαλή χρήση	Οι τελικοί χρήστες προστατεύουν τις έξυπνες κάρτες, tokens και pin και αισθάνονται ότι η πλαστογραφία είναι αδύνατη. Οι χρήστες τηρούν τις διαδικασίες και τα μέτρα διασφάλισης της ασφάλειας του συστήματος.	Εύκολοι στη χρήση και ανθεκτικοί στην παραποίηση μηχανισμοί, νομικές/κανονιστικές ποινές για ανάρμοστη χρήση, εκστρατεία ενημέρωσης των χρηστών, ενημέρωση για τα μέτρα και τις διαδικασίες ασφάλειας με μηνύματα βάσει συγκειμένου.
59	Ευκολία πρόσβασης σε απαραίτητα υλικά και υπηρεσίες	Οι τελικοί χρήστες έχουν εύκολη πρόσβαση σε υλικά και μπορούν να κάνουν τις αιτήσεις για την έξυπνες κάρτες σε μικρή απόσταση .	Λίαν διαδεδομένα σημεία προμήθειας/παροχής υλικών και υπηρεσιών (ΚΕΠ, δήμοι, δημόσιες αρχές ως εντεταλμένα γραφεία), ηλεκτρονικές πωλήσεις.
60	Κόστος και προαπαιτούμενα υλικών ή/και χρήσης του συστήματος	Το κόστος του τελικού χρήστη είναι χαμηλό, ή τουλάχιστον σε σύγκριση με τις υπηρεσίες που παρέχονται και το κόστος που αποφεύγει από τη χρήση του συστήματος.	Χρηματοδότηση έξυπνων καρτών, υλικών και ηλεκτρονικών υπηρεσιών από την κυβέρνηση και ευρωπαϊκά κονδύλια, απλές και σύντομες διαδικασίες πιστοποίησης και

			απόκτησης.
61	Ποιότητα διεπαφής προσωπικού υπηρεσίας / τελικού χρήστη – ύπαρξη καλώς ορισμένων, αποτελεσματικών διαδικασιών, ευκολία πρόσβασης (επίπεδο τελικού χρήστη)	Ο χρήστης έχει εύκολη πρόσβαση σε αυτοματοποιημένη και σε επανδρωμένη υποστήριξη, καθώς και σε επιγραμμική (online) βοήθεια.	Σύστημα επιγραμμικής, επανδρωμένης, αυτοματοποιημένης και χειροκίνητης βοήθειας.
62	Ικανότητες επικοινωνίας του προσωπικού υπηρεσίας – επηρεάζει σημαντικά την άποψη των χρηστών για το σύστημα (επίπεδο τελικού χρήστη)	Οι χρήστες πιστεύουν ότι το προσωπικό υπηρεσίας και υποστήριξης διαθέτει επαρκείς γνώσεις και διάθεση για να τους καθοδηγήσει αποτελεσματικά σε οποιεσδήποτε δυσκολίες ή προβλήματα αντιμετωπίσουν.	Εκπαίδευση προσωπικού υποστήριξης, τόσο στο προς υποστήριξη έργο, όσο και στις ικανότητες επικοινωνίας. Παροχή κινήτρων προς το προσωπικό υποστήριξης. Ορισμός διαδικασιών και κανόνων επικοινωνίας και υποστήριξης. Διασφάλιση ποιότητας μέσω αντικειμενικής και ανάλογα με τα αποτελέσματα αξιολόγησης.
63	Ικανοποίηση των προσδοκιών των χρηστών	Οι χρήστες αισθάνονται ότι η λειτουργικότητα του συστήματος είναι πλήρης και ολοκληρωμένη και ικανοποιεί τις ανάγκες τους.	Επισκόπηση και ανάλυση των προσδοκιών των χρηστών με πολλαπλές μεθόδους. Πιλοτικές εγκαταστάσεις του συστήματος σε επιλεγμένες ομάδες χρηστών. Έρευνα ικανοποίησης χρηστών.
64	Θέματα πολυγλωσσίας πολυπολιτισμικότητας	Ξένες και μειονοτικές ομάδες αισθάνονται καλά με τη χρήση του συστήματος.	Υλοποίηση του γραφικού περιβάλλοντος διαπροσωπείας εργασίας και βοήθειας σε τοπικές και ξένες γλώσσες.
65	Πίστη στα κίνητρα και στους τεθειμένους στόχους του συστήματος από την πολιτική ηγεσία (επίπεδο τελικού χρήστη)	Οι χρήστες έχουν εμπιστοσύνη ότι οι σκοποί και οι στόχοι του συστήματος που έχουν κοινοποιηθεί/προωθηθεί από την πολιτική ηγεσία αληθεύουν. Έχουν θετική παρελθούσα εμπειρία από την ίδια πολιτική ηγεσία.	Εκστρατεία ενημέρωσης και προβολής του έργου και άλλων παλαιότερων και αντίστοιχων. Κίνητρα προς τα ΜΜΕ για την προβολή της χρησιμότητας. Διαφανείς διαδικασίες και παρουσίαση του έργου.
ΣΤ	***Κοινωνικό επίπεδο***		
66	Ανατροπή εξουσιών και ισορροπιών λόγω νέων τεχνολογιών και γνώσης – δημιουργία φραγμάτων, κλειστών ομάδων και ανταγωνισμού (κοινωνικό επίπεδο)	Το ίδιο το έργο, οι υπηρεσίες, οι αρμοδιότητες, οι τεχνολογίες και η προβολή που εισάγει/προκαλεί δεν προκαλούν ανατροπή εξουσιών, αρμοδιοτήτων και ισορροπιών, φραγμούς, κλειστές ή προνομιούχες ομάδες και επιζήμιο ανταγωνισμό στις κοινωνικές ομάδες που απευθύνονται.	Ειδική ανάλυση και σχεδιασμός για την αντιμετώπιση θεμάτων εξουσιών, αρμοδιοτήτων και ισορροπιών, στις φάσεις επιχειρηματικής τοποθέτησης, προκήρυξης και υλοποίησης του έργου. Δημιουργία ομάδας εργασίας στο επίπεδο της διοίκησης για την εποπτεία και την αντιμετώ-

		Αντίθετα, λειτουργούν ως μέσα προώθησης κοινού συμφέροντος, ωφελημάτων, τεχνολογικής αναβάθμισης, συνεργασίας, ομοψυχίας και αρμονικής συνύπαρξης.	πιση προβλημάτων αυτού του είδους. Δημιουργία καναλιού επικοινωνίας με την πολιτική ηγεσία και τις κοινωνικές ομάδες και φορείς για την αντιμετώπιση τέτοιων προβλημάτων, σε όλες τις φάσεις του έργου. Έμφαση στην πρόληψη, αντί της εκ των υστέρων αντιμετώπισης.
67	Διείσδυση σε κλειστές ή απομονωμένες κοινωνικές ομάδες στόχου (πχ. εθνότητες, μειονότητες, φύλο, αγροτικές, νομαδικές)	Ειδικές ομάδες πληθυσμού, όπως εθνότητες, μειονότητες, ΑΜΕΑ κτλ. αισθάνονται ότι το έργο/σύστημα είναι φιλικό, εξυπηρετικό και σχεδιασμένο (και) γι' αυτές και έχουν κίνητρα για τη χρήση του.	Εκστρατεία ενημέρωσης ειδικών ομάδων πιθανών χρηστών ως προς τα οφέλη και τη σχεδίαση του έργου/συστήματος προς αυτές. Παροχή ειδικών κινήτρων και ειδική σχεδίαση και υλοποίηση του συστήματος για να λαμβάνονται υπόψη ιδιαιτερότητες και απαιτήσεις αυτών. Χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.
68	Πίστη στα κίνητρα και στους τεθειμένους στόχους του συστήματος από την πολιτική ηγεσία (κοινωνικό επίπεδο)	Το ευρύτερο κοινό και η κοινωνία έχουν πίστη και εμπιστοσύνη στα κίνητρα και τους στόχους που έχουν τεθεί από την πολιτική ηγεσία, τόσο για το παρελθόν του περιβάλλοντος του έργου, όσο και για το μέλλον και τα αποτελέσματα αυτού. Πιστεύουν επίσης ότι οι στόχοι που έχουν τεθεί και τα αναμενόμενα αποτελέσματα θα είναι προς όφελός τους, αλλά και του ίδιου του οργανισμού φορέα και των στόχων του.	Η πολιτική ηγεσία έχει επιδείξει σταθερή προσήλωση στους στόχους, στην ολοκλήρωση και στα αποτελέσματα του έργου, έχει ιστορικά πείσει σε παρόμοια ή συμπληρωματικά έργα, προς τελικό όφελος των οργανισμών, των φορέων και του ευρύτερου κοινού στο οποίο απευθύνεται το έργο. Ενημέρωση της πολιτικής ηγεσίας και της διοίκησης για την πολιτική που πρέπει να επιδείξουν και τις ενέργειας που πρέπει να κάνουν, προς όφελος του έργου, των σκοπών του και της θετικής άποψης του κοινού προς αυτό. Εκστρατεία ενημέρωσης του κοινού για τα οφέλη του έργου και την προσήλωση της πολιτικής ηγεσίας προς αυτά.
69	Θετική ψυχολογία μάζας προς το έργο και ανταπόκρισή του σε κοινωνικές ανάγκες, συνθήκες και κουλτούρα	Η ψυχολογία μάζας της κοινωνίας και του κοινού είναι θετικά προδιατεθειμένη προς το έργο/σύστημα. Πιστεύουν ότι θα συμβάλει θετικά στη ζωή και στην καθημερινότητά τους και έχουν εμπιστοσύνη στους στόχους του και τα κίνητρα αυτών που το προωθούν.	Μακροχρόνια εκστρατεία ενημέρωσης και πειθούς του κοινού για τα οφέλη του έργου και την ανταπόκρισή του στις κοινωνικές ανάγκες και συνθήκες. Χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης. Προσανατολισμός, στοχοθέτηση και σχεδίαση του

			έργου ώστε να ανταποκρίνεται κατά το δυνατό σε προσδοκίες, ανάγκες. συνθήκες, κουλτούρα και πεποιθήσεις του κοινού. Διαχρονικά επίδειξη ειλικρίνειας και ανταπόκρισης στις προσδοκίες του κοινού ,του οργανισμού φορέα και της πολιτικής ηγεσίας. Ανίχνευση και αντιμετώπιση παραγόντων που αντίκεινται στους στόχους, τη λειτουργία και την επιτυχία του έργου. Πιστοποίηση του συστήματος και των διαδικασιών που εφαρμόζει από αρχή προστασίας δεδομένων προσωπικού χαρακτήρα ή/και φορείς ελέγχου και πιστοποίησης ασφάλειας. Χρήση μηχανισμών ανθεκτικών στην παραποίηση. Χρήση υλικών με διεθνείς πιστοποιήσεις ασφάλειας. Χρήση τρίτων οργανισμών ή αναδόχων με πιστοποίηση ποιότητας διαδικασιών ή ασφάλειας. Ενημέρωση των χρηστών για τα χαρακτηριστικά ασφάλειας εντός των μεθόδων εξοικείωσης με το σύστημα. Κανονιστικό και νομικό πλαίσιο που προάγει την ασφάλεια και την αποτρέπει την αποκήρυξη ευθύνης
70	Επαρκής και θετική κάλυψη του έργου από τα ΜΜΕ	Τα ΜΜΕ προβάλλουν και προωθούν το έργο, διότι ανταποκρίνεται στα συμφέροντά τους, αποτελεί ενδιαφέρον θέμα για το κοινό, βελτιώνει τις κοινωνικές συνθήκες και βοηθά στην τεχνολογική πρόοδο, γνώση και κουλτούρα του κοινού. Η πολιτική ηγεσία, η διοίκηση και το αντικείμενο του έργου είναι προσφιλή στα ΜΜΕ και ταιριάζουν με τους εμπορικούς στόχους τους.	Προβολή και προώθηση του έργου προς τα ΜΜΕ και παροχή κινήτρων για την προβολή του. Ανάπτυξη διαπροσωπικών σχέσεων της πολιτικής ηγεσίας και της διοίκησης του φορέα του έργου με τα ΜΜΕ. Προσανατολισμός των στόχων του έργου σύμφωνα με τα πιστεύω των ΜΜΕ για τα συμφέροντα και τις επιθυμίες της κοινωνίας.
Ζ	***Επίπεδο προϋπαρχόντων πολιτικών/διαδικασιών***		
71	Συμβατότητα με υπάρχουσες πολιτικές και διαδικασίες	Το έργο είναι συμβατό λειτουργικά και στοχοπροσανατολισμένα με υπάρχουσες πολιτικές και διαδι-	Ανάλυση προϋπαρχόντων πολιτικών, κανονισμών και διαδικασιών του περιβάλλοντος του έργου. Σχεδίαση και

		κασίες του φορέα, του ευρύτερου νομικού, κανονιστικού και λειτουργικού περιβάλλοντός του, της κυβερνητικής πολιτικής και της κοινωνίας γενικότερα.	υλοποίηση με στόχο τη συμβατότητα με προϋπάρχουσες πολιτικές, διαδικασίες, κανονισμούς, λειτουργικότητα και πρότυπα του φορέα υλοποίησης, του νομικού, κανονιστικού και λειτουργικού περιβάλλοντος, της κυβερνητικής πολιτικής και πρακτικής.
72	Σχεδιασμός για ταχεία απόκριση σε μη αναμενόμενα θέματα πολιτικών/διαδικασιών	Το έργο διαθέτει την ευελιξία και την ταχεία απόκριση σε απρόβλεπτα θέματα μη συμβατότητας και δυσλειτουργίας με πολιτικές και διαδικασίες του περιβάλλοντός του.	Πρόβλεψη και υλοποίηση διαδικασιών και φορέα αντιμετώπισης απρόβλεπτων προβλημάτων συμβατότητας και δυσλειτουργίας. Ανασχεδιασμός προϋπαρχόντων πολιτικών, διαδικασιών και λειτουργικότητας, όπου απαιτείται για την επίτευξη των στόχων του έργου.
Η	***Νομικό/κανονιστικό επίπεδο***		
73	Εκ των προτέρων μελέτη νομικής/κανονιστικής συμμόρφωσης	Το έργο έχει σχεδιαστεί και υλοποιηθεί σύμφωνα με ειδική μελέτη νομικής και κανονιστικής συμμόρφωσης, έτσι ώστε να μειωθούν στο ελάχιστο προβλήματα τέτοιου είδους στην παραγωγική του λειτουργία.	Πρόβλεψη και υλοποίηση μελέτης κανονιστικής και νομικής συμμόρφωσης του έργου. Υλοποίησή του με βάση αυτή τη μελέτη και αξιολόγηση συμμόρφωσης στη λειτουργική φάση. Αξιολόγηση συμμόρφωσης από τρίτους ελεγκτικούς φορείς σε όλες τις φάσεις του έργου.
74	Νομικός/κανονιστικός εναρμονισμός μεταξύ χωρών	Το έργο υλοποιείται εντός συμβατού με άλλες χώρες κανονιστικού και νομικού περιβάλλοντος και σύμφωνα με αυτό.	Του έργου έχει προηγηθεί νομικός και κανονιστικός εναρμονισμός μεταξύ χωρών, όπου απαιτείται. Έγκαιρη ενημέρωση και ενέργειες προς/από την πολιτική ηγεσία για τον εναρμονισμό. Δημιουργία (όπου δεν υπάρχουν) και χρήση καναλιών επικοινωνίας με διεθνείς οργανισμούς/φορείς για την προώθηση της εναρμόνισης.
75	Επίσημη και ξεκάθαρη ανάθεση αρμοδιοτήτων	Σαφής και ορθή ανάθεση αρμοδιοτήτων στους φορείς και το προσωπικό που εμπλέκεται για όλες τις φάσεις του έργου. Δεν υπάρχουν εμπόδια και αντιθέσεις από κοινές αρμοδιότητες ή έλλειψη αυτών.	Ανάλυση αναγκών αρμοδιοτήτων του έργου για όλες τις φάσεις του. Αντιμετώπιση νομικών και κανονιστικών θεμάτων αρμοδιότητας. Έγκαιρη ανάθεση στους φορείς και το προσωπικό, όπως απαιτείται. Πρόβλεψη ανταπόκριση και προσαρμογή σε απρόβλεπτα προβλήματα αρμοδιότητας.
76	Προσαρμογή νομικού/κανονιστικού πλαι-	Το νομικό και κανονιστικό πλαίσιο έχει προσαρμοστεί,	Ανάλυση νομικών και κανονιστικών προσαρμογών απα-

	σίου στις ανάγκες του έργου	όπου αυτό κρίνεται απαραίτητο και όχι το αντίστροφο, στις απαιτήσεις για την εύρυθμη και χωρίς εμπόδια υιοθέτηση και λειτουργία του έργου και την επίτευξη των στόχων αυτού. Απρόβλεπτα εμπόδια αντιμετωπίζονται έγκαιρα και άμεσα.	ραίτητων για την υιοθέτηση και λειτουργία του έργου σε όλο το περιβάλλον υλοποίησης και λειτουργίας του. Έγκαιρη επικοινώνηση και εφαρμογή των προσαρμογών, πριν την παραγωγική λειτουργία. Πρόβλεψη και ανταπόκριση σε απρόβλεπτα προβλήματα προσαρμογής.
77	Ρυθμιστικό πλαίσιο λειτουργίας και εφαρμογή του από προσωπικό υπηρεσίας και χρήστες	Το έργο λειτουργεί εντός πλήρους και σαφούς ρυθμιστικού πλαισίου, το οποίο αποτελεί αρωγή και όχι τροχοπέδη στην εύρυθμη και αποτελεσματική λειτουργία του.	Ανάλυση αναγκών ρυθμιστικού πλαισίου, σύμφωνα με τις απαιτήσεις του έργου. Έγκαιρη επικοινώνηση και υλοποίηση του πλαισίου, όπου δεν υπάρχει, αλλαγή υπάρχοντος όπου υπάρχει και χρειάζεται. Ευελιξία για την άμεση αλλαγή του πλαισίου, προκειμένου να αντιμετωπιστούν απρόβλεπτες ανάγκες. Διασφάλιση ότι το πλαίσιο θα αποτελεί αρωγή και όχι τροχοπέδη στην εύρυθμη λειτουργία του έργου, βελτιώνοντας την ασφάλεια και τις διαδικασίες, χωρίς να εμποδίζει τη λειτουργικότητα.
78	Τοποθέτηση και αλληλεπίδραση εντός/με εθνικών πολιτικών και βραχυ/μεσοπρόθεσμων εθνικών στρατηγικών (νομικό/κανονιστικό επίπεδο)	Το έργο έχει τοποθετηθεί και αλληλεπιδρά (ή υπηρετεί) με θετικό τρόπο εθνικές και βραχυ/μεσοπρόθεσμες εθνικές στρατηγικές.	Εξαρχής σχεδίαση επιχειρηματικής περίπτωσης με στόχο την ένταξη εντός και την εξυπηρέτηση των εθνικών πολιτικών και στρατηγικών. Πρόβλεψη ανταπόκρισης και προσαρμογής σε απρόβλεπτες αλλαγές στις πολιτικές και στρατηγικές, χωρίς την απαξίωση ή την εγκατάλειψη του έργου.
79	Σχεδιασμός για ταχεία απόκριση σε μη αναμενόμενα νομικά και κανονιστικά θέματα	Έχουν προβλεφθεί και υλοποιηθεί διαδικασίες και φορείς για την άμεση απόκριση, αντίδραση και προσαρμογή σε απρόβλεπτα εμπόδια νομικής ή κανονιστικής φύσεως, εθνικού ή διεθνούς επιπέδου.	Πρόβλεψη, σχεδίαση και λειτουργία δομών άμεσης απόκρισης, αντίδρασης και προσαρμογής σε απρόβλεπτα εμπόδια νομικής ή κανονιστικής φύσεως, εθνικού ή διεθνούς επιπέδου. Δημιουργία (όπου δεν υπάρχουν) και χρήση καναλιών επικοινωνίας με την διοίκηση και την πολιτική ηγεσία για την εξυπηρέτηση αυτών των διαδικασιών.
Θ	***Οικονομικό επίπεδο***		
80	Σχεδιασμός και ανάπτυξη επιχειρηματι-	Το έργο είναι τοποθετημένο και στοχευμένο σε σωστή,	Μελέτη οικονομικής σκοπιμότητας και διαβούλευση με

	κής περίπτωσης (οικονομικό επίπεδο)	δικαιολογημένη και επιτυχή επιχειρηματική περίπτωση, όσον αφορά τον οικονομικό τομέα, η οποία έχει αναπτυχθεί έτσι ώστε να ανταποκρίνεται σε πραγματικές οικονομοτεχνικές συνθήκες και ταιριάζει με το οικονομικό περιβάλλον του έργου και τις τρέχουσες συνθήκες.	ενδιαφερόμενους φορείς, ομάδες, χρήστες, σε συνδυασμό με τη γενικότερη μελέτη επιχειρηματικής περίπτωσης του έργου. Στοχοθετημένη, αιτιολογημένη και ακριβής οικονομική επιχειρηματική σχεδίαση, σε συνεργασία με συμμετέχοντες και ενδιαφερόμενους φορείς.
81	Κατάλληλη κατανομή προϋπολογισμού	Τα κονδύλια που έχουν προβλεφθεί για το έργο έχουν κατανεμηθεί ορθά για όλα τα στάδια και τα υποσυστήματά του, καθώς και τις υποστηρικτικές, εξαρτώμενες και προαπαιτούμενες δράσεις. Υπάρχει πρόβλεψη για έκτακτες μη προβλεπόμενες δαπάνες και διαδικασίες αντιμετώπισής τους.	Σύνταξη προϋπολογισμού κατά στάδια, χρόνο και τύπο εξόδων. Κάλυψη τόσο των φάσεων, αμοιβών και υλικών του έργου, όσο και υποστηρικτικών, εξαρτωμένων και προαπαιτούμενων δράσεων. Πρόβλεψη για έκτακτες, απρόβλεπτες δαπάνες και διαδικασίες αντιμετώπισής τους.
82	Διαχείριση και παρακολούθηση πιστώσεων/κεφαλαίων	Υπάρχει κεντρική διαχείριση και παρακολούθηση πιστώσεων/κεφαλαίων, έτσι ώστε να καλύπτονται όλες οι τακτικές και έκτακτες δαπάνες του έργου.	Ολοκληρωμένο σύστημα διαχείρισης και παρακολούθησης πιστώσεων και εξόδων, για όλους τους τύπους αμοιβών και υλικών. Ένταξη στο αντίστοιχο σύστημα του περιβάλλοντος του έργου. Πρόβλεψη για αντιμετώπιση έκτακτων δαπανών.
I	***Επίπεδο προμηθειών***		
83	Διαδικασίες έγκαιρων προμηθειών	Το έργο υποστηρίζεται από αποτελεσματικό σύστημα προμηθειών, με δυνατότητες πρόβλεψης ζήτησης, έτσι ώστε όλα τα απαιτούμενα υλικά να είναι έγκαιρα διαθέσιμα για να μην υπάρχουν καθυστερήσεις σε κανένα στάδιο του έργου. Κανάλια επικοινωνίας με τους προμηθευτές έτσι ώστε να μην υπάρχουν αστοχίες και λάθη στις προμήθειες.	Σχεδίαση και υλοποίηση αποτελεσματικού συστήματος προμηθειών, ή ένταξη σε υπάρχον, με δυνατότητες πρόβλεψης ζήτησης και αποτελεσματικά κανάλια επικοινωνίας με προμηθευτές. Εφ' όσον το έργο εντάσσεται σε επιδοτούμενα ή μεγαλύτερα έργα, έγκαιρες και αποτελεσματικές διαδικασίες προαπαιτούμενων και αλληλεπιδράσεων.
84	Διαχείριση αποθήκης, εφοδιαστικής αλυσίδας και υλικού	Το έργο υποστηρίζεται από αποτελεσματικό σύστημα διαχείρισης αποθήκης και εφοδιαστικής αλυσίδας, έτσι ώστε όλα τα απαιτούμενα υλικά να είναι πάντα διαθέσιμα για να μην υπάρχουν καθυστερήσεις σε κανένα στάδιο του έργου.	Σχεδίαση και υλοποίηση συστήματος διαχείρισης αποθήκης ή/και εφοδιαστικής αλυσίδας, ή ένταξη σε υπάρχουσα. Εφ' όσον το έργο εντάσσεται στο πλαίσιο μεγαλύτερου, εκ των προτέρων προδιαγραφή και υλοποίηση έγκαιρων διαδικασιών εκπλήρωσης προαπαιτούμενων

			και αντιμετώπισης αλληλεπιδράσεων με αυτό.
ΙΑ	***Επίπεδο διαλειτουργικότητας***		
85	Χρήση ειδικής εφαρμογής παρακολούθησης και διαχείρισης της ολοκλήρωσης των τεχνολογιών εντός του έργου	Η ολοκλήρωση των τεχνολογιών του έργου γίνεται συντεταγμένα και με ειδικό σχεδιασμό, έτσι ώστε να μειώνονται οι πιθανότητες προβλημάτων και ασυμβατοτήτων, διασφαλίζοντας τη βέλτιστη λειτουργία των συστημάτων.	Υλοποίηση ειδικού σχεδίου ή εφαρμογής (ή ένταξη σε υπάρχουσα), παρακολούθησης και διαχείρισης της ολοκλήρωσης και της διαλειτουργικότητας των τεχνολογιών και των υποσυστημάτων του έργου. Πρόβλεψη για αντιμετώπιση μη αναμενόμενων προβλημάτων.
86	Ύπαρξη και συμμόρφωση με πρότυπα διαλειτουργικότητας	Το έργο και τα υποσυστήματά του είναι συμβατά με εθνικά ή διεθνή πρότυπα διαλειτουργικότητας, διασφαλίζοντάς την με άλλα έργα ή συστήματα που προϋπάρχουν ή υλοποιούνται παράλληλα ή ακολουθιακά, αυξάνοντας ταυτόχρονα την εμπιστοσύνη των φορέων και του κοινού προς το έργο.	Σχεδιασμός, υλοποίηση και πιστοποίηση του έργου και των υποσυστημάτων του με εθνικά ή διεθνή πρότυπα διαλειτουργικότητας. Επικοινώνηση αυτού προς τους φορείς, την πολιτική ηγεσία και τα ΜΜΕ.
87	Συμβατότητα προς τα πίσω με υπάρχοντα συστήματα και συμβατότητα προς τα μπρος με σχεδιαζόμενα μελλοντικά συστήματα	Το έργο και τα υποσυστήματά του είναι συμβατά προς τα πίσω με υπάρχοντα συστήματα και προς τα μπρος με σχεδιαζόμενα μελλοντικά, έτσι ώστε τόσο αυτό, όσο και εκείνα να λειτουργούν με βέλτιστο τρόπο. Μετατροπές δεδομένων και διαδικασιών, όπου απαιτούνται, είναι καλώς ορισμένες και δεν αποτελούν εμπόδιο για τη ομαλή λειτουργία, συνεργασία και επικοινωνία μεταξύ των έργων. Όπου υπάρχουν προαπαιτούμενα και εξαρτήσεις, είναι καλώς ορισμένα και έχουν ικανοποιηθεί.	Ένταξη ειδικής πρόβλεψης, σχεδιασμού και υλοποίησης για τη διαλειτουργικότητα σε όλα στα στάδια του έργου και ιδιαίτερα στη σύνταξη των προδιαγραφών και στη διαβούλευση με τους μελλοντικούς αναδόχους. Επαρκής γι' αυτό το στόχο ανάλυση και τεκμηρίωση όλων των προϋπαρχόντων συστημάτων. Μακροπρόθεσμος σχεδιασμός, με βάση καλώς ορισμένα πρότυπα, για τις προδιαγραφές τρεχόντων και μελλοντικών συστημάτων. Διασφάλιση καναλιών επικοινωνίας γι' αυτό το σκοπό με τη διοίκηση, τους αναδόχους και τους φορείς του έργου. Διασφάλιση επαρκούς τεχνικού επιπέδου του προσωπικού παρακολούθησης και παραλαβής και του αναδόχου για την επίτευξη της διαλειτουργικότητας. Διαδικασίες ελέγχου και πιστοποίησης διαλειτουργικότητας, πριν την παραγωγική φάση του έργου, καθώς και αντιμετώπισης απρόβλεπτων προβλημάτων.

88	Σχεδιασμός, παρακολούθηση και έλεγχος μετάπτωσης δεδομένων από συστήματα προς αντικατάσταση	Τα δεδομένα από υπάρχοντα συστήματα προς μετάπτωση στα νέα συστήματα του έργου μεταφέρονται χωρίς προβλήματα, με δυνατότητες ανάκλησης και αντιγράφων ασφάλειας.	Ένταξη ειδικής μελέτης, σχεδιασμού, υλοποίησης, ελέγχου και παρακολούθησης μετάπτωσης δεδομένων σε όλες τις φάσεις του έργου. Πρόβλεψη για δυνατότητες ανάκλησης αλλαγών και αντιγράφων ασφάλειας. Τεκμηρίωση διαδικασίας μετάπτωσης και επικοινώνηση αυτής προς τη διοίκηση και το προσωπικό υπηρεσίας του έργου.
89	Μελέτη και πρόβλεψη συνεργασίας, μεταφοράς/ανταλλαγής δεδομένων, εξαρτήσεων και βηματοδότησης υλοποίησης (implementation pacing) με άλλα έργα	Το έργο είναι ενταγμένο, συνεργάζεται και ανταλλάσει δεδομένα με άλλα έργα του περιβάλλοντός του χωρίς προβλήματα. Όπου υπάρχουν εξαρτήσεις και βηματοδότηση υλοποίησης, αυτές έχουν προδιαγραφεί, χρονοπρογραμματιστεί και υλοποιηθεί έτσι ώστε να μην προκαλούν εμπόδια στην υλοποίηση και τη λειτουργία αυτού και άλλων έργων. Η συνεργασία των επιτροπών παρακολούθησης και παραλαβής, της διοίκησης και του προσωπικού υπηρεσίας γίνεται χωρίς εμπόδια.	Πρόβλεψη και μελέτη συνεργασίας και μεταφοράς ή ανταλλαγής δεδομένων με άλλα έργα του περιβάλλοντος του έργου. Εξέταση και αντιμετώπιση θεμάτων εξάρτησης και βηματοδότησης υλοποίησης με άλλα έργα και αντίστοιχος χρονοπρογραμματισμός ενεργειών και διαδικασιών υλοποίησης. Επικοινωνία και συνεργασία επιτροπών παρακολούθησης και παραλαβής, διοίκησης και προσωπικού υπηρεσίας μεταξύ των έργων. Δημιουργία, όπου είναι δυνατό, κεντρικού συντονισμού των έργων. Χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διοίκησης.

Πίνακας 3. *Προτεινόμενες εξαρτήσεις μεταξύ κινδύνων και ενδεχόμενα εξάρτησης*

Στο οριζόντιο είναι ο επηρεαζόμενος κίνδυνος και στο κάθετο αυτός που τον επηρεάζει. Τόσο οι σχέσεις, όσο και τα ενδεχόμενα αποτελούν υλικό προς διευκόλυνση των αξιολογητών και δεν τους δεσμεύουν στο να τα προσαρμόσουν κατά την κρίση τους.

	3	11	18	20	21	22	26	28	31	33	37	39	42	48	49	50	52	53	55	56	57	58	63	65	66	67	68	74	75	76	77	78	79
1		0,50							0,60															0,70			0,70						
2		0,50																															
3			0,50																														
8						0,70																							0,80				
9					0,50		0,60																										
11				0,60				0,60																									
16	0,40										0,30												0,20		0,50	0,60							
17											0,30				0,50																		
18										0,50				0,50	0,65	0,65	0,70						0,80										
28																		0,75		0,90													
31													0,80																				
32												0,60																					
49																			0,70														
73																												0,50		0,70		0,50	0,70
76																						0,45									0,40		
77																				0,75	0,75												
80																					0,75												

Πίνακας 4. *Απόσπασμα της μήτρας RIPC[4] στο επίπεδο κινδύνου τελικού χρήστη στην ΥΔΚ-ΣΥΖΕΥΞΙΣ*

Σε αυτή την εφαρμογή δεν λαμβάνονται υπόψη αλληλεξαρτήσεις μεταξύ κινδύνων για το έργο.

Α/Α	Κίνδυνος	Επίπτωση	Πιθανότητα	ΚΠΕ	Αντίμετρα	Κόστος Αντιμέτρων	Κατώφλι Κάλυψης	Κάλυψη
53	Εξοικείωση με το έργο	8	0,7	Βασική γνώση των τελικών χρηστών για το αντικείμενο του έργου και το πως αυτό θα βελτιώσει τη ζωή τους και την αλληλεπίδρασή τους με την κυβέρνηση και τη δημόσια διοίκηση.	Εκστρατεία γνωριμίας και προώθησης του έργου, διαφημίσεις, διανομή φυλλαδίων, λευκά έγγραφα (white papers), χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.	6	7	8
54	Τεχνολογική κουλτούρα	6	0,7	Οι τελικοί χρήστες διαθέτουν βασική κατανόηση της σχετικής με το έργο τεχνολογίας, των διαδικασιών που ενέχει και των ωφελημάτων που προσφέρει.	Εύκολα προσβάσιμοι και ευκολο-κατανόητοι οδηγοί χρήσης, μέθοδοι τεχνολογικής διείσδυσης (πχ. συνεργασία με ISPs, σχολεία, εκθέσεις, μουσεία, τοπικές αρχές), χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.	8	5	6
55	Φιλικότητα χρήσης του συστήματος	7	0,4	Οι τελικοί χρήστες κατανοούν βασική πλοήγηση και διαδικασίες στο σύστημα, χωρίς την ανάγνωση υπερβολικής ποσότητας εγχειριδίων.	Εύκολο στην κατανόηση γραφικό περιβάλλον χρήσης με βοήθεια βάσει συγκειμένου (context sensitive help). Σχεδίαση της διαπροσωπείας του συστήματος βάσει απόψεων και δεξιοτήτων χρηστών ή αντιπροσωπευτικών ομάδων, καθώς και διεθνών προτύπων και βέλτιστων πρακτικών.	5	5	6
56	Εμπιστοσύνη προς το σύστημα, ιδιαίτερα όπου υπάρχει θέμα αποθήκευσης	10	0,6	Οι τελικοί χρήστες εμπιστεύονται τα προσωπικά τους δεδομένα και συναλλαγές στην αρχή που διαχειρίζεται ή/και χειρίζεται το	Πιστοποίηση του συστήματος και των διαδικασιών που εφαρμόζει από αρχή προστασίας δεδομένων ή/και φορείς ελέγχου ασφά-	5	8	10

	και χρήσης προσωπικών/ιδιωτικών δεδομένων			σύστημα.	λειας, χρήση μηχανισμών ανθεκτικών στην παραποίηση, χρήση υλικών με διεθνείς πιστοποιήσεις ασφάλειας, χρήση τρίτων οργανισμών ή αναδόχων με πιστοποίηση ποιότητας διαδικασιών ή ασφάλειας, ενημέρωση των χρηστών για τα χαρακτηριστικά ασφάλειας εντός των μεθόδων εξοικείωσης με το σύστημα, κανονιστικό και νομικό πλαίσιο που προάγει την ασφάλεια και την αποτρέπει την αποκήρυξη ευθύνης.			
57	Κίνητρα για χρήση (οικονομικά, χρονικά, ανάγκες)	9	0,7	Οι τελικοί χρήστες χρησιμοποιούν το σύστημα γιατί τους συμφέρει οικονομικά και χρονικά, σε σχέση με τη φυσική τους παρουσία ή τη χρήση μέσω τρίτων και τους παρέχονται περισσότερες δυνατότητες. Το έργο ανταποκρίνεται σε πραγματικές ανάγκες και επιθυμίες, ακόμα και αν αυτές είναι τεχνητές.	Εύκολη πρόσβαση σε ηλεκτρονικές υπηρεσίες που μειώνουν την ανάγκη για φυσική παρουσία, μικρότερες διαχειριστικές απαιτήσεις, πρόσβαση σε προωθημένες υπηρεσίες αν χρησιμοποιηθεί το σύστημα (πχ. έξυπνες κάρτες και υποδομή ΥΔΚ). Μελέτη σκοπιμότητας και επιχειρηματική τοποθέτηση του έργου ώστε να ανταποκρίνεται σε πραγματικές ανάγκες των ενδιαφερόμενων φορέων, ομάδων, χρηστών. Δημιουργία κινήτρων και αναγκών στους χρήστες (εφόσον οι πραγματικές δεν επαρκούν/υπάρχουν) μέσω των ΜΜΕ.	8	7	7
58	Κίνητρα για υπεύθυνη/ασφαλή χρήση	8	0,8	Οι τελικοί χρήστες προστατεύουν τις έξυπνες κάρτες, tokens και pin και αισθάνονται ότι η πλαστογραφία είναι αδύνατη	Εύκολοι στη χρήση και ανθεκτικοί στην παραποίηση μηχανισμοί, νομικές/κανονιστικές ποινές για ανάρμοστη χρήση, ενημέρωση χρηστών.	5	6	8
59	Ευκολία πρόσβασης σε απαραίτητα υλικά και υπηρε-	10	0,5	Οι τελικοί χρήστες έχουν εύκολη πρόσβαση σε υλικά και μπορούν να κάνουν τις αιτήσεις	Λίαν διαδεδομένα σημεία πώλησης (ΚΕΠ, δήμοι, δημόσιες αρχές ως εντεταλμένα γρα-	10	6	8

	σίες			για την έξυπνες κάρτες σε μικρή απόσταση .	φεία), ηλεκτρονικές πωλήσεις.			
60	Κόστος και προαπαιτούμενα υλικών ή/και χρήσης του συστήματος	10	0,4	Το κόστος του τελικού χρήστη είναι χαμηλό, ή τουλάχιστον σε σύγκριση με τις υπηρεσίες που παρέχονται και το κόστος που αποφεύγει από τη χρήση του συστήματος.	Χρηματοδότηση έξυπνων καρτών και ηλεκτρονικών υπηρεσιών από την κυβέρνηση και ευρωπαϊκά κονδύλια, απλές και σύντομες διαδικασίες πιστοποίησης και απόκτησης.	8	7	9
61	Ποιότητα διεπαφής προσωπικού υπηρεσίας / τελικού χρήστη – ύπαρξη καλώς ορισμένων, αποτελεσματικών διαδικασιών, ευκολία πρόσβασης (επίπεδο τελικού χρήστη)	8	0,5	Ο χρήστης έχει εύκολη πρόσβαση σε αυτοματοποιημένη και σε επανδρωμένη υποστήριξη, καθώς και σε επιγραμμική (online) βοήθεια.	Σύστημα επιγραμμικής, επανδρωμένης, αυτοματοποιημένης και χειροκίνητης βοήθειας.	6	5	8
62	Ικανότητες επικοινωνίας του προσωπικού υπηρεσίας – επηρεάζει σημαντικά την άποψη των χρηστώ για το σύστημα (επίπεδο τελικού χρήστη)	7	0,5	Το προσωπικό υπηρεσίας και υποστήριξης έχει επαρκείς γνώσεις και μπορεί να καθοδηγήσει αποτελεσματικά τους χρήστες σε οποιεσδήποτε δυσκολίες ή προβλήματα. Έχει κίνητρα για καλή υποστήριξη και καλώς ορισμένες διαδικασίες και κανονισμούς υποστήριξης.	Εκπαίδευση προσωπικού υποστήριξης, τόσο στο προς υποστήριξη έργο, όσο και στις ικανότητες επικοινωνίας. Παροχή κινήτρων προς το προσωπικό υποστήριξης. Ορισμός διαδικασιών και κανόνων επικοινωνίας και υποστήριξης και διασφάλιση ποιότητας μέσω αντικειμενικής και ανάλογα με τα αποτελέσματα αξιολόγησης.	7	5	6
63	Ικανοποίηση των προσδοκιών των χρηστών	6	0,4	Οι χρήστες αισθάνονται ότι η λειτουργικότητα του συστήματος είναι πλήρης και ολοκληρωμένη και συναντά τις ανάγκες τους για υπηρεσίες.	Επισκόπηση και ανάλυση των προσδοκιών των χρηστών με πολλαπλές μεθόδους, πιλοτικές εγκαταστάσεις του συστήματος σε επιλεγμένες ομάδες χρηστών, έρευνα ικανοποίησης χρηστών.	5	4	5
64	Θέματα πολυγλωσσίας πολυπολιτισμικότητας	7	0,5	Ξένες και μειονοτικές ομάδες αισθάνονται καλά με τη χρήση του συστήματος.	Υλοποίηση του γραφικού περιβάλλοντος διαπροσωπείας εργασίας και βοήθειας σε τοπικές και ξένες γλώσσες.	5	5	6

65	Πίστη στα κίνητρα και στους τεθειμένους στόχους του συστήματος από την πολιτική ηγεσία (επίπεδο τελικού χρήστη)	7	0,4	Οι χρήστες έχουν εμπιστοσύνη ότι οι σκοποί και οι στόχοι του συστήματος που έχουν κοινοποιηθεί/προωθηθεί από την πολιτική ηγεσία αληθεύουν, θετική παρελθούσα εμπειρία από την ίδια πολιτική ηγεσία.	Εκστρατεία ενημέρωσης και προβολής του έργου και άλλων παλαιότερων και αντίστοιχων, κίνητρα προς τα ΜΜΕ για την προβολή της χρησιμότητας, διαφανείς διαδικασίες και παρουσίαση του έργου.	8	5	5

Πίνακας 5. *Απόσπασμα της μήτρας RIPC[4] στην ΥΔΚ-ΣΥΖΕΥΞΙΣ με συνυπολογισμό αλληλεξαρτήσεων κινδύνων*

Σε αυτή την εφαρμογή λαμβάνονται υπόψη αλληλεξαρτήσεις κινδύνων, με υπολογισμό των πρότερων και μετέπειτα πιθανοτήτων που προκύπτουν από τις σχέσεις αλληλεξάρτησης.

A/A	Κίνδυνος	Επίπτωση	P_{pri}	P_{post}	ΚΠΕ	Αντίμετρα	Κόστος αντιμέτρων	Κατώφλι Κάλυψης	Κάλυψη
3	Κοινωνική και εμπορική τοποθέτηση και αιτιολόγηση (πόσο καλά τοποθετείται το έργο για να ανταποκριθεί και να καλύψει κοινωνικές και εμπορικές ανάγκες)		0,4						
11	Παρουσίαση, αιτιολόγηση και προώθηση του έργου στο προσωπικό κατώτερου κυβερνητικού/διοικητικού επιπέδου, στα ΜΜΕ και το ευρύ κοινό (πολιτικό επίπεδο)		0,4						
18	Λειτουργική, στόχο-προσανατολισμένη, με τεχνολογική επίγνωση και φιλική προς το χρήστη σύνταξη και επίβλεψη χαρακτηριστικών του έργου (διοικητικό επίπεδο)		0,5						
28	Παρουσίαση, αιτιολόγηση και προώθηση του έργου στο προσωπικό κατώτερου κυβερ-		0,55						

	νητικού/διοικητικού επιπέδου και το ευρύ κοινό (επίπεδο διοίκησης)								
49	Ακριβής υλοποίηση της επιχειρηματικής περίπτωσης, σχεδίασης και χαρακτηριστικών (επίπεδο αναδόχου/εργολάβου)		0,4						
53	Εξοικείωση με το έργο	8	0,7	0.9	Βασική γνώση των τελικών χρηστών για το αντικείμενο του έργου και το πως αυτό θα βελτιώσει τη ζωή τους και την αλληλεπίδρασή τους με την κυβέρνηση και τη δημόσια διοίκηση.	Εκστρατεία γνωριμίας και προώθησης του έργου, διαφημίσεις, διανομή φυλλαδίων, λευκά έγγραφα (white papers), χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.	6	7	8
54	Τεχνολογική κουλτούρα	6	0,7		Οι τελικοί χρήστες διαθέτουν βασική κατανόηση της σχετικής με το έργο τεχνολογίας, των διαδικασιών που ενέχει και των ωφελημάτων που προσφέρει.	Εύκολα προσβάσιμοι και ευκολοκατανόητοι οδηγοί χρήσης, μέθοδοι τεχνολογικής διείσδυσης (πχ. συνεργασία με ISPs, σχολεία, εκθέσεις, μουσεία, τοπικές αρχές), χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης.	6	5	6
55	Φιλικότητα χρήσης του συστήματος	7	0,4	0.46	Οι τελικοί χρήστες κατανοούν βασική πλοήγηση και διαδικασίες στο σύστημα, χωρίς την ανάγνωση υπερβολικής ποσότητας εγχειριδίων.	Εύκολο στην κατανόηση γραφικό περιβάλλον χρήσης με βοήθεια βάσει συγκειμένου (context sensitive help). Σχεδίαση της διαπροσωπείας του συστήματος βάσει απόψεων και δεξιοτήτων χρηστών ή αντιπροσωπευτικών ομάδων, καθώς και διεθνών προτύπων και βέλτιστων πρακτικών.	5	5	6

56	Εμπιστοσύνη προς το σύστημα, ιδιαίτερα όπου υπάρχει θέμα αποθήκευσης και χρήσης προσωπικών/ιδιωτικών δεδομένων	10	0,6	0.84	Οι τελικοί χρήστες εμπιστεύονται τα προσωπικά τους δεδομένα και συναλλαγές στην αρχή που διαχειρίζεται ή/και χειρίζεται το σύστημα.	Πιστοποίηση του συστήματος και των διαδικασιών που εφαρμόζει από αρχή προστασίας δεδομένων ή/και φορείς ελέγχου ασφάλειας, χρήση μηχανισμών ανθεκτικών στην παραποίηση, χρήση υλικών με διεθνείς πιστοποιήσεις ασφάλειας, χρήση τρίτων οργανισμών ή αναδόχων με πιστοποίηση ποιότητας διαδικασιών ή ασφάλειας, ενημέρωση των χρηστών για τα χαρακτηριστικά ασφάλειας εντός των μεθόδων εξοικείωσης με το σύστημα, κανονιστικό και νομικό πλαίσιο που προάγει την ασφάλεια και την αποτρέπει την αποκήρυξη ευθύνης.	5	8	10
57	Κίνητρα για χρήση (οικονομικά, χρονικά, ανάγκες)	9	0,7	0.94	Οι τελικοί χρήστες χρησιμοποιούν το σύστημα γιατί τους συμφέρει οικονομικά και χρονικά, σε σχέση με τη φυσική τους παρουσία ή τη χρήση μέσω τρίτων και τους παρέχονται περισσότερες δυνατότητες. Το έργο ανταποκρίνεται σε πραγματικές ανάγκες και επιθυμίες, ακόμα και αν αυτές είναι τεχνητές.	Εύκολη πρόσβαση σε ηλεκτρονικές υπηρεσίες που μειώνουν την ανάγκη για φυσική παρουσία, μικρότερες διαχειριστικές απαιτήσεις, πρόσβαση σε προωθημένες υπηρεσίες αν χρησιμοποιηθεί το σύστημα (πχ. έξυπνες κάρτες και υποδομή ΥΔΚ). Μελέτη σκοπιμότητας και επιχειρηματική τοποθέτηση του έργου ώστε να ανταποκρίνεται σε πραγματικές ανάγκες των ενδιαφερόμενων φορέων, ομάδων, χρηστών. Δημιουργία κινήτρων και αναγκών στους χρήστες (εφόσον οι πραγματικές δεν επαρκούν/υπάρχουν) μέσω των ΜΜΕ.	8	7	7

58	Κίνητρα για υπεύθυνη/ασφαλή χρήση	8	0,8	0.9	Οι τελικοί χρήστες προστατεύουν τις έξυπνες κάρτες, tokens και pin και αισθάνονται ότι η πλαστογραφία είναι αδύνατη	Εύκολοι στη χρήση και ανθεκτικοί στην παραποίηση μηχανισμοί, νομικές/κανονιστικές ποινές για ανάρμοστη χρήση, ενημέρωση χρηστών.	5	6	8
59	Ευκολία πρόσβασης σε απαραίτητα υλικά και υπηρεσίες	10	0,5		Οι τελικοί χρήστες έχουν εύκολη πρόσβαση σε υλικά και μπορούν να κάνουν τις αιτήσεις για την έξυπνες κάρτες σε μικρή απόσταση .	Λίαν διαδεδομένα σημεία πώλησης (ΚΕΠ, δήμοι, δημόσιες αρχές ως εντεταλμένα γραφεία), ηλεκτρονικές πωλήσεις.	10	6	8
60	Κόστος και προαπαιτούμενα υλικών ή/και χρήσης του συστήματος	10	0,4		Το κόστος του τελικού χρήστη είναι χαμηλό, ή τουλάχιστον σε σύγκριση με τις υπηρεσίες που παρέχονται και το κόστος που αποφεύγει από τη χρήση του συστήματος.	Χρηματοδότηση έξυπνων καρτών και ηλεκτρονικών υπηρεσιών από την κυβέρνηση και ευρωπαϊκά κονδύλια, απλές και σύντομες διαδικασίες πιστοποίησης και απόκτησης.	8	7	9
61	Ποιότητα διεπαφής προσωπικού υπηρεσίας / τελικού χρήστη – ύπαρξη καλώς ορισμένων, αποτελεσματικών διαδικασιών, ευκολία πρόσβασης (επίπεδο τελικού χρήστη)	8	0,5		Ο χρήστης έχει εύκολη πρόσβαση σε αυτοματοποιημένη και σε επανδρωμένη υποστήριξη, καθώς και σε επιγραμμική (online) βοήθεια.	Σύστημα επιγραμμικής, επανδρωμένης, αυτοματοποιημένης και χειροκίνητης βοήθειας.	6	5	8
62	Ικανότητες επικοινωνίας του προσωπικού υπηρεσίας – επηρεάζει σημαντικά την άποψη των χρηστώ για το σύστημα (επίπεδο τελικού χρήστη)	7	0,5		Το προσωπικό υπηρεσίας και υποστήριξης έχει επαρκείς γνώσεις και μπορεί να καθοδηγήσει αποτελεσματικά τους χρήστες σε οποιεσδήποτε δυσκολίες ή προβλήματα. Έχει κίνητρα για καλή υποστήριξη και καλώς ορισμένες διαδικασίες και κανονισμούς υποστήριξης.	Εκπαίδευση προσωπικού υποστήριξης, τόσο στο προς υποστήριξη έργο, όσο και στις ικανότητες επικοινωνίας. Παροχή κινήτρων προς το προσωπικό υποστήριξης. Ορισμός διαδικασιών και κανόνων επικοινωνίας και υποστήριξης και διασφάλιση ποιότητας μέσω αντικειμενικής και ανάλογα με τα αποτελέσματα αξιολόγησης.	7	5	6
63	Ικανοποίηση των προσδοκιών	6	0.5	0.9	Οι χρήστες αισθάνονται ότι η λειτουρ-	Επισκόπηση και ανάλυση των προσ-	5	4	5

	των χρηστών				γικότητα του συστήματος είναι πλήρης και ολοκληρωμένη και συναντά τις ανάγκες τους για υπηρεσίες.	δοκιών των χρηστών με πολλαπλές μεθόδους, πιλοτικές εγκαταστάσεις του συστήματος σε επιλεγμένες ομάδες χρηστών, έρευνα ικανοποίησης χρηστών.			
64	Θέματα πολυγλωσσίας πολυπολιτισμικότητας	7	0.4	0.45	Ξένες και μειονοτικές ομάδες αισθάνονται καλά με τη χρήση του συστήματος.	Υλοποίηση του γραφικού περιβάλλοντος διαπροσωπείας εργασίας και βοήθειας σε τοπικές και ξένες γλώσσες.	8	5	5
65	Προσαρμογή νομικού/κανονιστικού πλαισίου στις ανάγκες του έργου		0.4						
	Ρυθμιστικό πλαίσιο λειτουργίας και εφαρμογή του από προσωπικό υπηρεσίας και χρήστες		0.6						
	Σχεδιασμός και ανάπτυξη επιχειρηματικής περίπτωσης		0.7						

Πίνακας 6. *Απόσπασμα εφαρμογής της μεθόδου RIPC[4] σε πρωτότυπη ΥΔΚ*

Στον πίνακα αυτό παρουσιάζονται: α) για κάθε κίνδυνο, τα αποτελέσματα στο έργο που θα έχει στην περίπτωση πραγμάτωσής του, προκειμένου να υπολογιστεί η επίπτωσή του, β) οι παράγοντες που μπορεί να προκαλέσουν την πραγμάτωσή του, προκειμένου να υπολογιστεί η πιθανότητα, γ) οι τρωτότητες του έργου, προκειμένου να υπολογιστεί η κάλυψη των αντιμέτρων και δ) οι ΚΠΕ και τα αντίμετρα που τον αφορούν, επιλέγοντας από το υλικό της μεθοδολογίας RIPC[4]. Για λόγους χώρου, καταγράφονται μόνο οι κίνδυνοι στο πολιτικό επίπεδο.

Α/Α	Κίνδυνος	Παράγοντες πρόκλησής του (➔πιθανότητα)	Αποτελέσματα πραγμάτωσης (➔επίπτωση)	Σχετικές τρωτότητες του έργου (➔κάλυψη)	ΚΠΕ	Αντίμετρα
1	Υποστηριχτική αποφασιστικότητα και λήψη αποφάσεων	α) Η πολιτική ηγεσία δεν ενστερνίζεται την φιλοσοφία προστασίας των χρηστών. β) Η πολιτική ηγεσία δεν πιστεύει στη δυνατότητα της ΥΔΚ να πετύχει τους στόχους της. γ) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό διοίκησης του έργου.	Δυσχεραίνεται η ο σχεδιασμός, η χρηματοδότηση, η ανάθεση κατάλληλων αρμοδιοτήτων, η ολοκλήρωση του έργου και η επιτυχία των στόχων του σε πλάτος εφαρμογής και σε βάθος χρόνου.	α) Ανάγκη χρηματοδότησης για ανάπτυξη εφαρμογών εντός και εκτός (ως πελάτες) του έργου. β) Συντονισμός πολλών μερών για την σχεδίαση, την υλοποίηση και τη λειτουργία του έργου. γ) Ανάθεση κατάλληλων αρμοδιοτήτων και εξουσιών για όλες τις φάσεις του έργου.	Η πολιτική ηγεσία πιστεύει στο έργο και στη συμβολή του στο δημόσιο συμφέρον και την ΗΔ και είναι ενήμερη για τον απαιτούμενο χρονισμό και τη φύση των αποφάσεων και των βημάτων που απαιτούνται για την επιτυχία του έργου. Η εμπιστοσύνη και η υποστήριξη στο έργο είναι σταθερή και διακομματική ή/και επιβάλλεται από διεθνείς παράγοντες.	Βολιδοσκόπηση και αξιολόγηση των προθέσεων και των κινήτρων της πολιτικής ηγεσίας, επικοινώνηση των στόχων, των προτερημάτων, των πιθανών αποτελεσμάτων, των εμποδίων, των πιθανοτήτων επίτευξης των στόχων του έργου, παροχή κατάλληλων κινήτρων και επιχειρημάτων στην πολιτική ηγεσία, προς όφελος του έργου. Προϋπολογισμός κόστους για όλα τα στοιχεία του έργου, προβολή των αναγκών συντονισμού και συνεργασίας για την επιτυχή λειτουργία.
2	Μεσο/μακροπρόθεσμος	α) Η πολιτική ηγεσία δεν έχει ενιαία πολιτική και	Δυσλειτουργία ή και ακύρωση του έργου σε οποι-	α) μια ΥΔΚ απαιτεί σημαντική διαχρονική υπο-	Η πολιτική ηγεσία είναι διαχρονικά ενήμερη για τις φά-	Διαρκής ενημέρωση της πολιτικής ηγεσίας για τις φά-

	ενιαίος σχεδιασμός και δέσμευση στο έργο (πολιτικό επίπεδο)	άποψη για το έργο. Αντικρουόμενες απόψεις, στόχοι ή συμφέροντα. β) Η πολιτική ηγεσία δεν έχει θετική άποψη, ή εξοικείωση με το έργο. γ) Αλλαγή κυβέρνησης/πολιτικής ηγεσίας που προκαλεί αλλαγή στην υποστήριξη / σχεδιασμό. δ) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό διοίκησης του έργου.	οδήποτε φάση του, μη πραγμάτωση των στόχων του, μη ανάληψη των ενεργειών που αποτελούν προαπαιτούμενα για την επιτυχία, αποτυχία στην πρόβλεψη εμποδίων για την επιτυχή έκβαση.	στήριξη σε όλα τα επίπεδα (ηγεσία, διοίκηση, ανάδοχος, προσωπικό λειτουργίας, χρήστες). β) Συντονισμός πολλών μερών για την σχεδίαση, την υλοποίηση και τη λειτουργία της συγκεκριμένης ΥΔΚ. γ) Οι ΥΔΚ απαιτούν από τη φύση τους για την επιτυχία αντιμετώπιση εμποδίων που δεν έχουν προβλεφθεί (πχ. τεχνικά προβλήματα εντός του έργου, τεχνικά προβλήματα σε προαπαιτούμενα). δ) Η εμπιστοσύνη, βασικό σε μια ΥΔΚ, δομείται μακροπρόθεσμα. ε) Η συγκεκριμένη ΥΔΚ απαιτεί μακροχρόνιο σχεδιασμό και υποστήριξη λόγω πολύπλοκων διαδικασιών και πολλών μερών που ενέχονται.	σεις, την κατάσταση, τα προαπαιτούμενα, το χρονισμό, τη φύση των αποφάσεων και των βημάτων που απαιτούνται για την επιτυχία του έργου του έργου. Η εμπιστοσύνη και η υποστήριξη στο έργο είναι διακομματική ή/και επιβάλλεται από διεθνείς παράγοντες. Το έργο είναι ενταγμένο στο μεσο/μακρο-πρόθεσμο κυβερνητικό σχεδιασμό, ο οποίος δεν μεταβάλλεται από κυβέρνηση σε κυβέρνηση.	σεις, την κατάσταση, τα προαπαιτούμενα, το χρονισμό και τη φύση των αποφάσεων και των βημάτων που απαιτούνται για την επιτυχία του έργου, καθώς και των επιπτώσεων της αποτυχίας. Προβολή των ωφελημάτων του έργου σε κυβερνητικό, εθνικό, κομματικό και διακομματικό επίπεδο. Προβολή των τεχνολογιών του έργου ως μέσο προώθησης της κυβερνητικής πολιτικής και βελτίωσης της εικόνας του κυβερνητικού έργου. Προβολή των αναγκών συντονισμού και συνεργασίας για την ορθή λειτουργία του έργου. Προβολή των αναγκών και μεθόδων ανύψωσης της εμπιστοσύνης στην ΥΔΚ. Παροχή κινήτρων και επιχειρημάτων για την υποστήριξη του έργου, λόμπυινγκ (προώθηση) για το έργο. Όπου το έργο σχετίζεται με διεθνείς συνθήκες ή/και χρηματοδότηση, ενημέρωση της ηγεσίας για τις

						συνέπειες μη ολοκλήρωσης και χρήση του διεθνούς παράγοντα ως μόχλευση για την προώθηση του έργου. Ειδική πρόβλεψη για τη συνέχιση της υποστήριξης, της υλοποίησης και της λειτουργίας του έργου μετά από αλλαγή κυβέρνησης. Πρόβλεψη για την ένταξη του έργου στον κυβερνητικό σχεδιασμό και παροχή των προαπαιτούμενων γι' αυτό.
3	Κοινωνική και εμπορική τοποθέτηση και αιτιολόγηση (πόσο καλά τοποθετείται το έργο για να ανταποκριθεί και να καλύψει κοινωνικές και εμπορικές ανάγκες)	α) έλλειψη εναρμονισμού της αντίληψης της πολιτικής ηγεσίας με τις πραγματικές κοινωνικές ή εμπορικές ανάγκες. β) λανθασμένη αντίληψη της ηγεσίας για την σωστή ολοκλήρωση, λειτουργικότητα και διάρθρωση του έργου για την κάλυψη των αναγκών. γ) Ανεπαρκής τοποθέτηση, αιτιολόγηση και προβολή του έργου στην κοινωνία και την οικονομία από την πολιτική ηγεσία.	α) το έργο δεν ανταποκρίνεται σε πραγματικές ανάγκες ή ανταποκρίνεται σε λάθος ανάγκες της κοινωνίας και της οικονομίας. β) το έργο δεν έχει αιτιολογηθεί και προωθηθεί σωστά στη δημόσια διοίκηση και στην κοινωνία. Τελικό αποτέλεσμα: έλλειψη ανταπόκρισης και εμπιστοσύνης στο έργο, μικρή διείσδυση του έργου.	α) η συγκεκριμένη ΥΔΚ αποτελεί πρωτοποριακό σχεδιασμό που απαιτεί σε ιδιαίτερο βαθμό εμπιστοσύνη και υποστήριξη για την υιοθέτηση της, ενέχοντας αναγκαστικά σχετικά πολύπλοκες διαδικασίες και τεχνολογίες. β) η συγκεκριμένη ΥΔΚ απαιτεί ταίριασμα των πιστεύω των εμπλεκομένων φορέων και της πολιτικής ηγεσίας με τη φιλοσοφία της.	Το έργο τοποθετείται και λειτουργεί κατάλληλα και επαρκώς για να καλύψει υπάρχουσες κοινωνικές και εμπορικές ανάγκες, με την υποστήριξη της πολιτικής ηγεσίας. Η ολοκλήρωσή του φτάνει σε σημείο λειτουργικότητας και διάθρωσης ώστε να καλύπτει πραγματικούς σκοπούς, ανάγκες και απαιτήσεις.	Καθοδήγηση, έλεγχος και αξιολόγηση, πριν, κατά και μετά την ολοκλήρωση του έργου έτσι ώστε να εξασφαλίζονται οι απαιτήσεις τοποθέτησης και λειτουργίας του και των ιδιαιτεροτήτων του. Έρευνα σε στοχευόμενους χρήστες και μη, χρησιμότητας και τοποθέτησης του έργου, τόσο κατά τη φάση δοκιμαστικής λειτουργίας, όσο και στην κανονική λειτουργία του. Χρήση διαδραστικών τεχνολογιών ενημέρωσης, ηλεκτρονικής διακυ-

						βέρνησης, ΜΜΕ και δημοσκοπήσεων.
4	Υποστήριξη για/από άλλες συμπληρωματικές ή ακολουθιακές πολιτικές και έργα (πολιτικό επίπεδο)	α) έλλειψη κανονιστικού και νομικού πλαισίου για την εισαγωγή και τη λειτουργία (ΔΠΠ) της υποδομής. β) έλλειψη έργων-πελατών της υπηρεσίας. γ) έλλειψη υποστηρικτικής, εκπαιδευτικής, και προωθητικής πολιτικής. δ)) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό σχεδιασμού και διοίκησης του έργου.	α) δυσχέρειες στη λειτουργία του έργου, από απλά λειτουργικά θέματα μέχρι νομικά/κανονιστικά εμπόδια. β) ακόμα και αν φτάσει σε φάση λειτουργίας θα είναι άλλο ένα έργο που θα γίνει μόνο για να γίνει, χωρίς ουσιαστική συνεισφορά στη ανάπτυξη της ΗΔ, προς όφελος της κοινωνίας, της οικονομίας και των πολιτών.	α) η συγκεκριμένη ΥΔΚ αποτελεί πρωτοποριακό σχεδιασμό που απαιτεί σε ιδιαίτερο βαθμό εμπιστοσύνη και υποστήριξη για την υιοθέτηση της, ενέχοντας αναγκαστικά σχετικά πολύπλοκες διαδικασίες και τεχνολογίες. β) Ως ΥΔΚ, αποτελεί υπηρεσία προς άλλες υπηρεσίες και η έλλειψη υπηρεσιών-πελατών (=κινήτρων προς χρήση) ακυρώνει τη χρησιμότητά της. γ) Ως ΥΔΚ πρέπει να πλαισιώνεται από συμπληρωματικές ή ακολουθιακές πολιτικές και έργα που να υποστηρίζουν και να ενισχύουν τη χρησιμότητά της.	Το έργο είναι τοποθετημένο σε πολιτικό και λειτουργικό περιβάλλον ευνοϊκό για την ολοκλήρωση και λειτουργία του και πλαισιώνεται από άλλα έργα που το συμπληρώνουν και το υποστηρίζουν. Τα έργα αυτά ολοκληρώνονται σύμφωνα με τις απαιτήσεις του υπό εξέταση έργου, έτσι ώστε να μην δημιουργούν εμπόδια.	Προώθηση κεντρικού πολιτικού σχεδιασμού που ευνοεί το υπό εξέταση έργο, κατανόηση και υπόδειξη των εξαρτήσεων του έργου από πολιτικές και άλλα έργα, προώθηση των υπό εξάρτηση έργων. Πρόβλεψη για τη δημιουργία μίας τουλάχιστον δημοφιλούς εφαρμογής-πελάτη για την προώθηση της ΥΔΚ. Πρόβλεψη για αντιμετώπιση απρόβλεπτων/έκτακτων καταστάσεων.
5	Κουλτούρα τεχνολογίας της πολιτικής ηγεσίας	α) η πολιτική ηγεσία δεν διαθέτει την κατάλληλη κουλτούρα για να καταλάβει τη χρησιμότητα του	Δυσχέρειες στην προώθηση του έργου και στην αντιμετώπιση προβλημάτων και εμποδίων στο	Το συγκεκριμένο έργο, και σαν ΥΔΚ, αλλά και λόγω του ιδιαίτερου χαρακτήρα και φιλοσοφίας	Η πολιτική ηγεσία διαθέτει τεχνολογική αίσθηση και άποψη, κατανοεί την τεχνολογική διάσταση του έργου,	Επιμόρφωση και ενημέρωση της πολιτικής ηγεσίας, λόμπυινγκ (προώθηση) για το έργο, χρήση διαδραστικών

		έργου και να αισθανθεί εγγύτητα με αυτό. β) η πολιτική ηγεσία δεν πλαισιώνεται από προσωπικό με την δυνατότητα και ικανότητα να προωθήσει τα ανωτέρω.	κανονιστικό/νομικό πλαίσιο, στον προγραμματισμό, στη χρηματοδότηση, τη σχεδίαση και την υλοποίηση.	του, είναι ευάλωτο στην έλλειψη τεχνολογικής κουλτούρας της ηγεσίας που θα το προωθήσει.	συνδέει την τεχνολογική με την πολιτική/κοινωνική διάσταση και χρησιμότητα του έργου	τεχνολογιών ενημέρωσης και ηλεκτρονικής διακυβέρνησης, υποστήριξη από τα ΜΜΕ.
6	Εξοικείωση της πολιτικής ηγεσίας με το έργο (σε υψηλό επίπεδο)	α) η πολιτική ηγεσία δεν διαθέτει την κατάλληλη εξοικείωση με το έργο ώστε να το προωθήσει αποτελεσματικά και να αντιμετωπίσει εγκαίρως προβλήματα και προαπαιτούμενα για την επιτυχία του. β) η πολιτική ηγεσία δεν πλαισιώνεται από προσωπικό με την δυνατότητα και ικανότητα να το προωθήσει αποτελεσματικά και να αντιμετωπίσει εγκαίρως προβλήματα και προαπαιτούμενα για την επιτυχία του. γ) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό σχεδιασμού και διοίκησης του έργου.	Δυσχέρειες στην προώθηση του έργου και στην αντιμετώπιση προβλημάτων και εμποδίων στο κανονιστικό/νομικό πλαίσιο, στον προγραμματισμό, στη χρηματοδότηση και την υλοποίηση.	Το συγκεκριμένο έργο, και σαν ΥΔΚ, αλλά και λόγω του διαφορετικού χαρακτήρα, φιλοσοφίας, συνεργατικότητας και συντονισμού που χρειάζεται, είναι ιδιαίτερα ευάλωτο στην έλλειψη εξοικείωσης της ηγεσίας που θα το προωθήσει.	Η πολιτική ηγεσία διαθέτει επαρκή γνώση για τη πολιτική, κοινωνική, επιχειρηματική, οικονομική και τεχνολογική χρησιμότητα του έργου, τις τεχνολογίες που εισάγει (σε υψηλό επίπεδο), καθώς και των απαιτήσεων για την ολοκλήρωση και την επίτευξη των στόχων του.	Κατάλληλη επιμόρφωση και ενημέρωση της πολιτικής ηγεσίας, λόμπυινγκ (προώθηση) για το έργο, κατανόηση και υπόδειξη των εξαρτήσεων του έργου από πολιτικές και άλλα έργα, προώθηση των τεχνολογιών του έργου ως μέσο προώθησης της κυβερνητικής πολιτικής και βελτίωσης της εικόνας του κυβερνητικού έργου.
7	Επαρκής και	α) έλλειψη εξοικείωσης	Οι απαιτήσεις σε τεχνικό	α) το έργο εξαρτάται από	Το έργο διαθέτει διαχρονικά	Όπου αυτό εξαρτάται από

	διαχρονική κατανομή πιστώσεων (υψηλό στρατηγικό επίπεδο)	της πολ. ηγεσίας με τα οικονομικά προαπαιτούμενα, τον προγραμματισμό και την τρέχουσα κατάσταση του έργου. β) έλλειψη εμπράγματης υποστήριξης στους στόχους και τη φιλοσοφία του έργου. γ) γενική έλλειψη πόρων, είτε αντικειμενικά, είτε λόγω κακού προγραμματισμού και οργάνωσης. δ) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό σχεδιασμού και διοίκησης του έργου.	επίπεδο, συνεργασίας μεταξύ φορέων και προμήθειας υλικών είναι τέτοιες γι' αυτή την ΥΔΚ που έλλειψη έγκαιρων και επαρκών πιστώσεων θα έχει σαν αποτέλεσμα πλήρη αποτυχία του έργου, ή τουλάχιστον εξαιρετική αργοπορία στην υλοποίηση.	τις κατάλληλες πιστώσεις για τις ΑΠ, ΑΕξ και ΕΤΑ, οι οποίες βασίζονται σε εμπορικές ΥΔΚ. β) η συγκεκριμένη ΥΔΚ απαιτεί μη τετριμμένη ανάπτυξη λογισμικού για την υλοποίηση των ΕΠΕ και ΕΠΧ των ΕΤΑ, ΑΕξ και ΟΑ. γ) η ΥΔΚ βασίζεται στην προμήθεια και διανομή έξυπνων καρτών.	τις απαραίτητες πιστώσεις για την ολοκλήρωσή του και την επίτευξη των στόχων του.	εθνικές συνθήκες, έγκαιρος προγραμματισμός και προϋπολογισμός· όπου εξαρτάται από διεθνείς συνθήκες, κατάλληλη ανταπόκριση στα εθνικά προαπαιτούμενα και επικοινώνηση της κατάστασης ανάπτυξης και ολοκλήρωσης του έργου. Ειδική πρόβλεψη, προϋπολογισμός και κατανομή πιστώσεων για την ανάπτυξη του απαιτούμενου λογισμικού. Αξιολόγηση των αναδόχων για αποτελεσματική απορρόφηση κονδυλίων έρευνας και ανάπτυξης.
8	Κατανομή αρμοδιότητας/δικαιοδοσίας μεταξύ κυβερνητικών υπηρεσιών	α) έλλειψη εξοικείωσης της πολ. ηγεσίας με τα προαπαιτούμενα, τον προγραμματισμό και την τρέχουσα κατάσταση του έργου. β) έλλειψη εμπράγματης υποστήριξης στους στόχους και τη φιλοσοφία του έργου. γ) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό σχεδιασμού και διοίκη-	α) Ως έργο ΥΔΚ με υψηλές απαιτήσεις συνεργασίας, μη σωστή κατανομή αρμοδιοτήτων αποτελεί σημαντικό κίνδυνο για την υλοποίηση και λειτουργία της ΥΔΚ. β) Μείωση της εμπιστοσύνης στην ΥΔΚ λόγω αντικρουόμενων αρμοδιοτήτων και εντάσεων, που μπορεί να προκαλέ-	α) η συγκεκριμένη ΥΔΚ βασίζεται σε στενή συνεργασία μεταξύ ΑΠ, ΕΤΑ, ΑΕξ και ΟΑ, τόσο για την ανάπτυξη του λογισμικού, όσο και για τη λειτουργία της. β) η ΥΔΚ περιλαμβάνει προαιρετικά τη χρήση ΕΓ για τις ΑΕξ και ΟΑ. γ) ανάμεσα στις ΑΠ, ΕΤΑ, ΑΕξ και ΟΑ πρέπει	Έχει εκχωρηθεί, νομικά, κανονιστικά ή διοικητικά στους φορείς που μετέχουν στα στάδια του έργου η κατάλληλη δικαιοδοσία, χωρίς να παρουσιάζονται εμπόδια από άλλους φορείς.	Έγκαιρη επικοινώνηση προς την πολιτική ηγεσία των αναγκών δικαιοδοσίας και συνεργασίας των φορέων που μετέχουν στο έργο, προκειμένου να ρυθμιστούν κατάλληλα τα νομικά, κανονιστικά και διοικητικά πλαίσια. Πρόβλεψη για μηχανισμό και διαδικασίες ταχείας αντιμετώπισης και επίλυσης στην περίπτωση που εμφανιστούν

		σης του έργου. δ) αντικρουόμενες απόψεις και συμφέροντα που σχετίζονται με το έργο, εντός της πολιτικής ηγεσίας.	σει μέχρι και πλήρη αποτυχία του έργου.	να υπάρχουν αμοιβαίες σχέσεις εμπιστοσύνης, προϋπόθεση των οποίων είναι η κατάλληλη κατανομή αρμοδιοτήτων.		προβλήματα δικαιοδοσίας.
9	Τοποθέτηση και αλληλεπίδραση με/εντός εθνικών πολιτικών και βραχυ/μεσοπρόθεσμων εθνικών στρατηγικών (πολιτικό επίπεδο)	α) έλλειψη εξοικείωσης της πολ. ηγεσίας με τα προαπαιτούμενα, τον προγραμματισμό, τους στόχους και τα οφέλη του έργου. β) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό σχεδιασμού και διοίκησης του έργου. γ) αντικρουόμενες απόψεις και συμφέροντα που σχετίζονται με το έργο, εντός της πολιτικής ηγεσίας. δ) έλλειψη ενιαίου και κεντρικού προγραμματισμού και στρατηγικής, εντός της πολ. ηγεσίας, για τις δημόσιες επενδύσεις και την εθνική στρατηγική.	α) Ως έργο ΥΔΚ είναι ευαίσθητο σε κακή τοποθέτηση και αλληλεπίδραση με εθνικές πολιτικές και στρατηγικές και μπορεί να οδηγηθεί σε αχρηστία, ακόμα και αν φτάσει σε λειτουργία. β) Εμπόδια στη συνεργασία και λειτουργία της ΥΔΚ που μπορεί να μειώσουν την εμπιστοσύνη των εμπλεκομένων προς αυτή.	α) η ΥΔΚ βασίζεται σε φιλοσοφία προστασίας των προσωπικών δεδομένων και εμπιστοσύνης από τους εμπλεκόμενους φορείς και το στοχευόμενο κοινό. Αυτά μπορούν να οικοδομηθούν μόνο με ένταξη και θετική αλληλεπίδραση της ΥΔΚ με εθνικές πολιτικές και στρατηγικές. β) η συνεργασία μεταξύ των φορέων, βασική για την υλοποίηση και λειτουργία της ΥΔΚ μπορεί να επιτευχθεί μόνο με ένταξη και θετική αλληλεπίδραση της ΥΔΚ με εθνικές πολιτικές και στρατηγικές.	Το έργο είναι σύμφωνο και αλληλεπιδρά θετικά με εθνικές πολιτικές και στρατηγικές και είναι ανθεκτικό σε αλλαγές αυτών, διότι ανταποκρίνεται σε διαχρονικές, πραγματικές εθνικές, κοινωνικές, οικονομικές ανάγκες.	Σωστός επιχειρηματικός, πολιτικός, οικονομικός και κοινωνικός σχεδιασμός του έργου, ευελιξία των στόχων και των απαιτήσεών του σε μεταβλητό πολιτικό και εθνικό περιβάλλον, σωστή επικοινωνία και λόμπυινγκ του έργου προς την ηγεσία. Προσαρμογή των εθνικών πολιτικών και στρατηγικών, όπου αυτό είναι δυνατό.
10	Τοποθέτηση και αλληλεπίδραση του	α) έλλειψη εξοικείωσης της πολ. ηγεσίας με τα προαπαιτούμενα, την	α) Ως έργο ΥΔΚ είναι ευαίσθητο σε κακή τοποθέτηση και αλληλεπίδρα-	α) η ΥΔΚ βασίζεται σε φιλοσοφία προστασίας των προσωπικών δεδο-	Το έργο είναι σύμφωνο και αλληλεπιδρά θετικά με διεθνείς περιφερειακές και κε-	Σωστός επιχειρηματικός σχεδιασμός του έργου σε σχέση με άλλα διεθνή έργα,

	έργου με περιφερειακές και κεντρικές διεθνείς οδηγίες, πολιτικές και έργα (πολιτικό επίπεδο)	τοποθέτηση, τους στόχους και τα οφέλη του έργου. β) έλλειψη εξοικείωσης της πολτικής ηγεσίας με περιφεριακές και κεντρικές διεθνείς οδηγίες, πολιτικές και έργα που σχετίζονται με το έργο. γ) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό σχεδιασμού και διοίκησης του έργου. δ) έλλειψη ενιαίου και κεντρικού προγραμματισμού και στρατηγικής, εντός της πολ. ηγεσίας, για τις δημόσιες επενδύσεις και την εθνική και διεθνή στρατηγική.	ση με περιφερειακές και κεντρικές διεθνείς οδηγίες, πολιτικές, στρατηγικές και έργα και μπορεί να οδηγηθεί σε αχρηστία, ακόμα και αν φτάσει σε λειτουργία. β) Εμπόδια στη συνεργασία και λειτουργία της ΥΔΚ που μπορεί να μειώσουν την εμπιστοσύνη των εμπλεκομένων προς αυτή.	μένων και εμπιστοσύνης από τους εμπλεκόμενους φορείς και το στοχευόμενο κοινό. Για τα ανωτέρω δεν πρέπει να τίθενται εμπόδια από περιφερειακές και κεντρικές διεθνείς οδηγίες, πολιτικές και έργα. β) δεν πρέπει να υπάρχουν εμπόδια από περιφερειακές και κεντρικές διεθνείς οδηγίες, πολιτικές και έργα για τη συνεργασία μεταξύ των φορέων που συμμετέχουν και συνεργάζονται στα πλαίσια του έργου.	ντρικές πολιτικές, στρατηγικές, οδηγίες και έργα και είναι ανθεκτικό σε αλλαγές αυτών, διότι ανταποκρίνεται σε διαχρονικές, πραγματικές εθνικές και διεθνείς ανάγκες.	ευελιξία των στόχων και των απαιτήσεών του σε μεταβλητό πολιτικό και εθνικό περιβάλλον, σωστή επικοινωνία και λόμπυινγκ του έργου.
11	Παρουσίαση, αιτιολόγηση και προώθηση του έργου στο προσωπικό κατώτερου κυβερνητικού/διοικητικού επιπέδου, στα ΜΜΕ και	α) έλλειψη εξοικείωσης της πολ. ηγεσίας με τα προαπαιτούμενα, την τοποθέτηση, τους στόχους και τα οφέλη του έργου. β) έλλειψη εμπράγματης υποστήριξης στους στόχους και τη φιλοσοφία του έργου. γ) αντικρουόμενες απόψεις	α) μείωση της αποτελεσματικότητας και του στοχοπροσανατολισμού του μεσαίου και κατώτερου κυβερνητικού/ διοικητικού προσωπικού που μπορεί να οδηγήσει σε μείωση του συντονισμού και της αποτελεσματικότητα που χρειάζονται για	α) ως ΥΔΚ, αλλά και λόγω της ιδιάζουσας φύσης της, είναι ευαίσθητη στην ύπαρξη υψηλού επίπεδου εμπιστοσύνης, προώθησης της φιλοσοφίας της και της συνέργιας που ενέχει η λειτουργία της από το προσωπικό των εμπλεκομένων φορέων,	Με ενέργειες της ηγεσίας, το έργο είναι γνωστό και κατανοητό, όσον αφορά τους στόχους του, τις ανάγκες, τα στάδια, τη χρησιμότητα και την κατάστασή του, στο κατώτερο κυβερνητικό και διοικητικό προσωπικό και στο ευρύ κοινό	Διαχρονική υποστήριξη του έργου από την πολιτική ηγεσία, κατάλληλη επικοινώνηση και προώθησή του με τρόπο που να αφομοιώνεται εύκολα από το κατώτερο κυβερνητικό/διοικητικό επίπεδο και το ευρύ κοινό. Χρήση διαδραστικών τεχνολογιών ενημέρωσης και ηλε-

	το ευρύ κοινό (πολιτικό επίπεδο)	και συμφέροντα που σχετίζονται με το έργο, εντός της πολιτικής ηγεσίας. δ) Η πολιτική ηγεσία δεν ενστερνίζεται την φιλοσοφία της και δεν πιστεύει στη δυνατότητα της ΥΔΚ να πετύχει τους στόχους της. ε) η έννοια της προστασίας των προσωπικών δεδομένων είναι αντίθετη με εμπορικές και διοικητικές πολιτικές που εφαρμόζονται και έρχονται σε πλήρη αντίθεση με τη φιλοσοφία της συγκεκριμένης ΥΔΚ.	την επιτυχή ολοκλήρωση και λειτουργία της ΥΔΚ. β) μη επαρκής προβολή στα ΜΜΕ μπορεί να μειώσει σημαντικά την εμπιστοσύνη των φορέων και του κοινού στην ΥΔΚ και να μην προάγει τα ιδιαίτερα χαρακτηριστικά της και τα οφέλη τους. γ) μικρή διείσδυση στο στοχευόμενο κοινό (οργανισμοί και ιδιώτες).	των ΜΜΕ και το κοινό. β) συνήθεις πολιτικές, εμπορικές και διοικητικές πρακτικές έρχονται σε πλήρη αντίθεση με τη φιλοσοφία της συγκεκριμένης ΥΔΚ.		κτρονικής διακυβέρνησης. Ειδικά για τα ΜΜΕ, προσέγγιση και προβολή του έργου με κατάλληλο τρόπο, γειτνίασή του με τα συμφέροντά τους, ένταξή του στη γενικότερη προωθητική προσπάθεια της κυβέρνησης, δημιουργία κινήτρων και αναγκών στους χρήστες (εφόσον τα πραγματικά δεν επαρκούν/υπάρχουν) μέσω των ΜΜΕ.
12	Οικονομικές, διοικητικές και διαπροσωπικές σχέσεις (όπου σχετίζονται και μπορούν να επηρεάσουν το έργο) με τοπικές και εθνικές οικονομικές και παραγωγι-	α) η πολιτική ηγεσία δεν επικοινωνεί ή/και δεν μοιράζεται τους στόχους, τη φιλοσοφία και τις ανάγκες τοπικών και εθνικών παραγωγικών δυνάμεων και πολιτών που ενστερνίζονται και ωφελούνται από μια ΥΔΚ που προστατεύει το προσωπικό απόρρητο. Αυτό λειτουργεί και αντίστροφα. β) Η	α) μη επαρκής προβολή των ωφελημάτων της ΥΔΚ σε τοπικές και εθνικές οικονομικές και παραγωγικές δυνάμεις και ΜΜΕ που μπορεί να μειώσει την εμπιστοσύνη προς την ΥΔΚ και την υποστήριξη για τα ιδιαίτερα ωφελήματα που έχει να προσφέρει. β) μικρή διείσδυση στο	α) ως ΥΔΚ, αλλά και λόγω της ιδιάζουσας φύσης της, είναι ευαίσθητη στην ύπαρξη υψηλού επίπεδου εμπιστοσύνης, προώθησης της φιλοσοφίας της και της συνέργιας που ενέχει η λειτουργία της από τοπικές και εθνικές οικονομικές και παραγωγικές δυνάμεις και ΜΜΕ. β) συνήθεις πολιτικές,	Τοπικές και εθνικές οικονομικές και παραγωγικές δυνάμεις, όπως και τοπικά και εθνικά ΜΜΕ βλέπουν ωφελήματα από το έργο, είτε από την ανάπτυξή του είτε από τα αποτελέσματά του, είτε άμεσα, είτε έμμεσα, μέσω άλλων έργων.	Σωστή τοποθέτηση και επιχειρηματική σχεδίαση του έργου, λόμπυινγκ στους κατάλληλους παράγοντες και ΜΜΕ, παρουσίαση με τρόπο ώστε να κάνει το έργο απαραίτητο στη συνείδηση και στα συμφέροντά τους.

	κές δυνάμεις, εθνικά/τοπικά ΜΜΕ	φιλοσοφία της ΥΔΚ δεν συμβαδίζει με την φιλοσοφία και τα πιστεύω της πολ. ηγεσίας και σε συνδυασμό με το (α), με τα αντίστοιχα των παραγωγικών μονάδων.	στοχευόμενο κοινό(οργανισμοί και ιδιώτες).	εμπορικές και διοικητικές πρακτικές έρχονται σε πλήρη αντίθεση με τη φιλοσοφία της συγκεκριμένης ΥΔΚ.		
13	Οικονομικές, διοικητικές και πολιτικές σχέσεις και συνθήκες (που σχετίζονται και μπορούν να επηρεάσουν το έργο) με γειτονικές, περιφερειακές και κεντρικές κυβερνητικές, οικονομικές και παραγωγικές δυνάμεις, διεθνή ΜΜΕ	α) η πολιτική ηγεσία δεν επικοινωνεί ή/και δεν μοιράζεται τους στόχους, τη φιλοσοφία και τις ανάγκες με γειτονικές, περιφερειακές και κεντρικές κυβερνητικές, οικονομικές και παραγωγικές μονάδες που ενστερνίζονται και ωφελούνται από μια ΥΔΚ που προστατεύει το προσωπικό απόρρητο. Αυτό λειτουργεί και αντίστροφα. β) Η φιλοσοφία της ΥΔΚ δεν συμβαδίζει με την φιλοσοφία και τα πιστεύω της πολ. ηγεσίας και σε συνδυασμό με το (α), με τα αντίστοιχα των παραγωγικών μονάδων.	α) μη επαρκής προβολή των ωφελημάτων της ΥΔΚ σε γειτονικές περιφερειακές και κεντρικές κυβερνητικές οικονομικές και παραγωγικές δυνάμεις και ΜΜΕ που μπορεί να μειώσει την εμπιστοσύνη προς την ΥΔΚ και την υποστήριξη για τα ιδιαίτερα ωφελήματα που έχει να προσφέρει. β) μικρή διείσδυση στο στοχευόμενο κοινό (οργανισμοί και ιδιώτες).	α) ως ΥΔΚ, αλλά και λόγω της ιδιάζουσας φύσης της, είναι ευαίσθητη στην ύπαρξη υψηλού επίπεδου εμπιστοσύνης, προώθησης της φιλοσοφίας της και της συνέργιας που ενέχει η λειτουργία της από τοπικές και εθνικές οικονομικές και παραγωγικές δυνάμεις και ΜΜΕ. β) συνήθεις πολιτικές, εμπορικές και διοικητικές πρακτικές έρχονται σε πλήρη αντίθεση με τη φιλοσοφία της συγκεκριμένης ΥΔΚ.	Γειτονικές, περιφερειακές ή κεντρικές κυβερνητικές, οικονομικές ή παραγωγικές δυνάμεις και ΜΜΕ βλέπουν ωφελήματα από το έργο, είτε από την ανάπτυξή του είτε από τα αποτελέσματά του, είτε άμεσα, είτε έμμεσα, μέσω άλλων έργων.	Σωστή τοποθέτηση και επιχειρηματική σχεδίαση του έργου, λόμπυινγκ στους κατάλληλους παράγοντες και ΜΜΕ, παρουσίαση με τρόπο ώστε να κάνει το έργο απαραίτητο στη συνείδηση και στα συμφέροντά τους.
14	Πρόβλεψη, διασφάλιση	α) η πολιτική ηγεσία δεν επικοινωνεί ή/και δεν	α) προβλήματα στο σωστό σχεδιασμό, τοποθέ-	Η αυξημένη πολυπλοκότητα των διαδικασιών	Με πρωτοβουλία της πολιτικής ηγεσίας, η διοίκηση, οι	Παροχή κατάλληλων κινήτρων στην πολιτική ηγεσία

	και παρακολούθηση αποτελεσματικότητας ως προς την παροχή κινήτρων για την ορθή και υπεύθυνη υλοποίηση, λειτουργία και χρήση του έργου, προς τη διοίκηση, τους αναδόχους/εργολάβους, το προσωπικό υπηρεσίας και το κοινό στο οποίο απευθύνεται (πολιτικό επίπεδο)	μοιράζεται τους στόχους, τη φιλοσοφία και τις ανάγκες τοπικών και εθνικών παραγωγικών δυνάμεων και πολιτών που ενστερνίζονται και ωφελούνται από μια ΥΔΚ που προστατεύει το προσωπικό απόρρητο. β) έλλειψη εξοικείωσης της πολ. ηγεσίας με τα προαπαιτούμενα, την τοποθέτηση, τους στόχους και τα οφέλη του έργου. γ) Η φιλοσοφία της ΥΔΚ δεν συμβαδίζει με την φιλοσοφία και τα πιστεύω της πολ. ηγεσίας και σε συνδυασμό με τα αντίστοιχα υπολοίπων εμπλεκομένων. δ) ελλιπής επικοινωνία της ηγεσίας με το προσωπικό σχεδιασμού και διοίκησης του έργου.	τηση, υλοποίηση, ολοκλήρωση και λειτουργία της ΥΔΚ, με αποτελέσματα: εμπόδια στη συνεργασία μεταξύ φορέων, ιδιαίτερα σημαντικό για το συγκεκριμένο έργο, απειλές για την ασφάλεια και μείωση της εμπιστοσύνης προς αυτήν. β) μείωση της διείσδυσης στο στοχευόμενο κοινό (οργανισμοί και ιδιώτες).	που ενέχει σημαίνει ότι υπάρχει αυξημένη εξάρτηση της επιτυχούς ολοκλήρωσης, λειτουργίας και διείσδυσης της ΥΔΚ από κίνητρα που θα δοθούν στους εμπλεκόμενους φορείς και στις στοχευόμενες πλευρές. Τα κίνητρα που θα δοθούν πρέπει να είναι πραγματικά και να αντισταθμίζουν την ανωτέρω πολυπλοκότητα.	ανάδοχοι/εργολάβοι, το προσωπικό υπηρεσίας και το κοινό στο οποίο απευθύνεται το έργο έχουν τα κατάλληλα κίνητρα και κατανόηση ώστε να διοικήσουν, υλοποιήσουν, λειτουργήσουν και χρησιμοποιήσουν, αντίστοιχα, σωστά το έργο, προκειμένου να επιτύχει τους στόχους του και να έχει τα αναμενόμενα θετικά αποτελέσματα, τα οποία θα έχουν με τη σειρά τους θετικό αντίκτυπο στη γνώμη που έχουν οι παραπάνω για την πολιτική ηγεσία (κλείσιμο κύκλου). Κατανόηση από την ηγεσία των κινήτρων που πρέπει να έχουν οι υπόλοιποι προς όφελος του έργου.	για διαχρονική υποστήριξη και προώθηση του έργου, με απώτερο στόχο η επιτυχία του να έχει θετικό αντίκτυπο στη γνώμη των υπολοίπων προς αυτή. Καλλιέργεια της κατάλληλης εργοστραφούς κουλτούρας της ηγεσίας. Επικοινώνηση των κινήτρων που πρέπει να έχει το κατώτερο προσωπικό και το ευρύ κοινό προς όφελος της επίτευξης των στόχων και της ορθής λειτουργίας του έργου.

Πίνακας 7. *Απόσπασμα της μήτρας RIPC[4] στο πολιτικό επίπεδο σε πρωτότυπη ΥΔΚ*

Στον πίνακα αυτό παρουσιάζεται απόσπασμα εφαρμογής της μήτρας RIPC[4] στο πολιτικό επίπεδο της πρωτότυπης ΥΔΚ, με υπολογισμούς που εφαρμόζονται στα δεδομένα που παρουσιάστηκαν στον Πίνακα 6.

A/A	Κίνδυνος	Επίπτωση	Εξάρτηση από	Ppri	Ppost	Κόστος	Κατώφλι	Κάλυψη
1	Υποστηριχτική αποφασιστικότητα και λήψη αποφάσεων	6		0,15		5	4	6
2	Μεσο/μακρο-πρόθεσμος ενιαίος σχεδιασμός και δέσμευση στο έργο (πολιτικό επίπεδο)	8		0,25		7	6	8
3	Κοινωνική και εμπορική τοποθέτηση και αιτιολόγηση (πόσο καλά τοποθετείται το έργο για να ανταποκριθεί και να καλύψει κοινωνικές και εμπορικές ανάγκες)	10	16	0,3	0,36	6	7	9
4	Υποστήριξη για/από άλλες συμπληρωματικές ή ακολουθιακές πολιτικές και έργα (πολιτικό επίπεδο)	6		0,4		6	5	6
5	Κουλτούρα τεχνολογίας της πολιτικής ηγεσίας	6		0,2		4	5	5
6	Εξοικείωση της πολιτικής ηγεσίας με το έργο (σε	5		0,3		5	3	5

	υψηλό επίπεδο)							
7	Επαρκής και διαχρονική κατανομή πιστώσεων (υψηλό στρατηγικό επίπεδο)	10		0,2		5	7	7
8	Κατανομή αρμοδιότητας/δικαιοδοσίας μεταξύ κυβερνητικών υπηρεσιών	6		0,3		7	5	5
9	Τοποθέτηση και αλληλεπίδραση με/εντός εθνικών πολιτικών και βραχυ/μεσο-πρόθεσμων εθνικών στρατηγικών (πολιτικό επίπεδο)	7		0,2		5	5	6
10	Τοποθέτηση και αλληλεπίδραση του έργου με περιφερειακές και κεντρικές διεθνείς οδηγίες, πολιτικές και έργα (πολιτικό επίπεδο)	6		0,15		5	4	6
11	Παρουσίαση, αιτιολόγηση και προώθηση του έργου στο προσωπικό κατώτερου κυβερνητικού/διοικητικού επιπέδου, στα ΜΜΕ και το ευρύ κοινό (πολιτικό επίπεδο)	9	1 και 2	0,3	0,5	8	6	8
12	Οικονομικές, διοικητικές και διαπροσωπικές σχέ-	5		0,2		7	3	5

	σεις (όπου σχετίζονται και μπορούν να επηρεάσουν το έργο) με τοπικές και εθνικές οικονομικές και παραγωγικές δυνάμεις, εθνικά/τοπικά ΜΜΕ							
13	Οικονομικές, διοικητικές και πολιτικές σχέσεις και συνθήκες (που σχετίζονται και μπορούν να επηρεάσουν το έργο) με γειτονικές, περιφερειακές και κεντρικές κυβερνητικές, οικονομικές και παραγωγικές δυνάμεις, διεθνή ΜΜΕ	4		0,2		7	3	4
14	Πρόβλεψη, διασφάλιση και παρακολούθηση αποτελεσματικότητας ως προς την παροχή κινήτρων για την ορθή και υπεύθυνη υλοποίηση, λειτουργία και χρήση του έργου, προς τη διοίκηση, τους αναδόχους/εργολάβους, το προσωπικό υπηρεσίας και το κοινό στο οποίο απευθύνεται (πολιτικό επίπεδο)	9		0,5		10	7	8

16	Επαρκής σχεδίαση και αιτιολόγηση επιχειρηματικής περίπτωσης (business case development)			0,33				

Πίνακας 8. Ορισμοί συμβολισμών και συναρτήσεων για την πρωτότυπη ΥΔΚ

Στον πίνακα αυτό παρουσιάζονται οι συμβολισμοί που χρησιμοποιούνται στους αλγόριθμους και στις διαδικασίες της πρωτότυπης ΥΔΚ που περιγράφεται στο Κεφάλαιο 4, η οποία χρησιμοποιείται ως περίπτωση εφαρμογής της προτεινόμενης μεθοδολογίας ΑΔ.

Παρουσίαση	**Επεξήγηση**
(K_{Apu}, K_{Apr})	Ζεύγος ασύμμετρων κλειδιών της οντότητας *A*, δημόσιο και ιδιωτικό, μήκους τουλάχιστον 1024 bits.
(AK_{Apu}, AK_{Apr})	Ζεύγος ανώνυμων ασύμμετρων κλειδιών της οντότητας *A*, δημόσιο και ιδιωτικό, μήκους τουλάχιστον 1024 bits. Τεχνικά αυτά τα κλειδιά δεν διαφέρουν από τα μη-ανώνυμα.
At_A	Χαρακτηριστικό (τιμή) της οντότητας *A*. Στο μοντέλο αναφέρεται ως το Ειδικό για τον Οργανισμό Αναγνωριστικό (ΕΟΑ) ενός Οργανισμού Αποδέκτη (ΟΑ). Χρησιμοποιείται για να συσχετίσει μοναδικά την ταυτότητα της *A* με το λογαριασμό της στο πληροφοριακό σύστημα του ΟΑ.
$\bar{A}t_A = (K_{ROpu}, At_A)$	Ζεύγος χαρακτηριστικού της οντότητας *A*. Αποτελείται από το δημόσιο κλειδί ενός ΟΑ και την τιμή του χαρακτηριστικού.
Id_A	Η ταυτότητα της οντότητας *A*. Τυπικά αποτελείται από το όνομα και το επώνυμο ενός ατόμου. Λαμβάνεται ως δεδομένο ότι δεν επαρκεί για την μοναδική συσχέτιση του ατόμου με το λογαριασμό του στον ΟΑ ή για την απόδειξη της κατοχής ενός χαρακτηριστικού.
(UN_A, PW_A)	Απλά διαπιστευτήρια (όνομα, κωδικός) της οντότητας *A*. Λαμβάνεται ως δεδομένο ότι δεν αποτελούν απόδειξη ταυτότητας ή κατοχής ενός χαρακτηριστικού. Παράγονται τυπικά από τον ίδιο το χρήστη, μερικές φορές από τον ΟΑ. Χρησιμοποιούνται τυπικά για τον ελάχιστον συσχετισμό της συνεδρίας του χρήστη με τον λογαριασμό του στο πληροφοριακό σύστημα του ΟΑ.
A: *act*	Η ενέργεια *act* της οντότητας *A*.
A: $m \rightarrow B$	Το μήνυμα *m* στέλνεται από την οντότητα *A* στην οντότητα *B* με σύνδεση που διασφαλίζει την εμπιστευτικότητα (SSL/TLS).
A: $m \rightarrow B$	Το μήνυμα *m* περνάει με φυσική παρουσία από την οντότητα *A* στην *B*.
$m = (m_1, m_2)$	Το μήνυμα *m* αποτελείται από την ακολουθία m_1 και m_2.
$E_z(m)$	Κρυπτογράφηση του *m* με το συμμετρικό κλειδί *z* μήκους τουλάχιστον 256 bits. Προτεινόμενοι αλγόριθμοι: AES, Serpen, Twofish.
$D_z(c)$	Αποκρυπτογράφηση του *c* με το συμμετρικό κλειδί *z* μήκους τουλάχιστον 256 bits.
$E_{Apu}(m)$	Κρυπτογράφηση του *m* με το δημόσιο κλειδί της οντότητας *A*. Προτεινόμενος αλγόριθμος: RSAES-PKCS1-v1_5.

$D_{Apu}(c)$	Αποκρυπτογράφηση του *c* με το δημόσιο κλειδί της οντότητας *A*.
$E_{Apr}(m)$	Κρυπτογράφηση του *m* με το ιδιωτικό κλειδί της οντότητας *A*. Όταν γίνεται στην πλευρά του χρήστη, η κρυπτογράφηση γίνεται τυπικά από υλικό/λογισμικό εντός της Ασφαλούς Διάταξης Αποθήκευσης Πιστοποιητικών (ΑΔΑΠ), μετά από ερώτηση του pin. Το ιδιωτικό κλειδί δεν βγαίνει ποτέ εκτός της ΑΔΑΠ και δεν είναι γνωστό στην *A*. Προτεινόμενος αλγόριθμος: RSAES-PKCS1-v1_5.
$D_{Apr}(c)$	Αποκρυπτογράφηση του *c* με το ιδιωτικό κλειδί της οντότητας *A*. Όταν γίνεται στην πλευρά του χρήστη, η αποκρυπτογράφηση γίνεται από υλικό/λογισμικό εντός της ΑΔΑΠ, μετά από ερώτηση του pin. Το ιδιωτικό κλειδί δεν βγαίνει ποτέ εκτός της ΑΔΑΠ και δεν είναι γνωστό στην *A*.
$H(m)$	Ο μονο-κατευθυντικός κατατεμαχισμός του μηνύματος *m*. Προτεινόμενοι αλγόριθμοι: RIPEMD-160, SHA-2, WHIRLPOOL.
$s_m = \boldsymbol{S}_A(m)$	Η ψηφιακή υπογραφή του μηνύματος *m* με το ιδιωτικό κλειδί της οντότητας *A*; αποτελεί συνδυασμό κατακερματισμού και κρυπτογράφησης. Προτεινόμενοι αλγόριθμοι: RSASSA-PKCS1-v1_5, DSA. $\boldsymbol{S}_A(m) \Leftrightarrow (E_{Apr}(H(m))$
$m_s = S_A(m)$	Το (ψηφιακά) υπογεγραμμένο μήνυμα που αποτελείται από το μήνυμα *m* και την υπογραφή του με το ιδιωτικό κλειδί της οντότητας *A*. $S_A(m) \Leftrightarrow (m, \boldsymbol{S}_A(m))$
$V^?_A(m_s)$	Επαλήθευση του υπογεγραμμένου μηνύματος m_s με το δημόσιο κλειδί της οντότητας *A*. $\left[V_A^?(m_s) \Leftrightarrow \left(H(m') \stackrel{?}{=} D_{A_{publ}}(S_A(m))\right)\right] / \left[m_s \equiv (m', S_A(m))\right]$
NSK()	Συνάρτηση που παράγει ένα νέο κλειδί *z*. Μπορεί να δημιουργείται αυτόματα ή με ερώτηση στο χρήστη.
$(K_{Apu}, K_{Apr}) = NAK()$	Συνάρτηση που παράγει ένα νέο ζεύγος κλειδιών για την οντότητα *A*. Όταν γίνεται στην πλευρά του χρήστη, παράγεται τυπικά (και αποθηκεύεται) από υλικό/λογισμικό εντός της ΑΔΑΠ. Τυπικά προστατεύεται από ένα pin που ορίζεται από το χρήστη, ο οποίος ωστόσο, δεν μαθαίνει ποτέ το ιδιωτικό κλειδί. Τυπικά περιλαμβάνει μια περιγραφή, για φιλικότητα προς το χρήστη.
OTP()	Συνάρτηση που παράγει ένα κωδικό ή ακολουθία πλήρωσης μιας χρήσης, μήκους συγκεκριμένου αριθμού bits (τυπικά τουλάχιστον 128).
sn = *ESN*(*pkc*)	Εξαγωγή του σειριακού αριθμού του πιστοποιητικού ταυτότητας (ΠΤ) *pkc*.
$PKCR(Id_A, K_{Apu})$	Αίτηση πιστοποιητικού δημοσίου κλειδιού με το δημόσιο κλειδί της οντότητας *A* με ταυτότητα Id_A.

$ACR(cP_A, K_{Bpu})$	Αίτηση πιστοποιητικού χαρακτηριστικών (ACR) με το κρυπτο-ψευδώνυμο cP_A της οντότητας *A* και το δημόσιο κλειδί K_{Bpu} της οντότητας *B*.
$cb = nPKCb\ (PKCR(Id_A, K_{Apu}))$	Κατασκευή του σώματος *cb* (χωρίς ψηφιακή υπογραφή) νέου ΠΤ για την οντότητα *A*, από την αίτηση με ταυτότητα Id_A που κατέχει το δημόσιο κλειδί K_{Apu}. Βασικά πεδία: έκδοση, σειριακός αριθμός, αλγόριθμος υπογραφής, εκδότης, περίοδος ισχύος, αντικείμενο.
$acb = nACb\ (ACR(cP_A, K_{Bpu}), At_A))$	Κατασκευή του σώματος *acb* (χωρίς την ψηφιακή υπογραφή) νέου ΠΧ από την αίτηση για την οντότητα *A* που κατέχει το χαρακτηριστικό At_A που έχει εκδοθεί από την οντότητα *B* με δημόσιο κλειδί K_{Bpu}. Βασικά πεδία: έκδοση, κάτοχος, εκδότης, αλγόριθμος υπογραφής, σειριακός αριθμός, περίοδος ισχύος, χαρακτηριστικό.
$P_A = NRID()$	Κατασκευή νέου ψευδωνύμου για την οντότητα *A*.
$IC(c,K_{Apu})$	Εγκατάσταση εντός της ΑΔΑΠ πιστοποιητικού *c* με δημόσιο κλειδί K_{Apu} της οντότητας *A* και συσχέτισή του με το ζεύγος κλειδιών με το ίδιο δημόσιο κλειδί.

Η σελίδα αυτή είναι σκόπιμα λευκή

Δημοσιεύσεις – Εργασίες Συγγραφέα

1. Κεφαλληνός, Δ. και Συκάς, Ε. (2006) «Ανασκόπηση ερευνητικών θεμάτων ασφάλειας στα MANET», ΠΜΣ, Ε.Μ.Π.
2. Kefallinos, D., Lambrou, M.A., Sykas, E.D. (2006) 'Secure PKI-enabled E-Government Infrastructures Implementation: the SYZEFXIS-PKI Case', *Electronic Government International Journal*, 3(4), pp. 420-438
3. Κεφαλληνός, Δ. και Συκάς, Ε. (2007) «Τεχνικές ανίχνευσης επισυνδέσεων με χρήση υπέρτερης γνώσης προσβλητότητας και δομημένων πληροφοριών κατάστασης και γεγονότων» , ΠΜΣ, Ε.Μ.Π.
4. Kefallinos, D., Lambrou, M.A., Sykas, E.D. (2009) 'An Extended Risk Assessment Model for Secure E-Government Projects', *International Journal of Electronic Government Research,* 5(2), pp. 72-92
5. Kefallinos, D. Lambrou. M.A., Sykas, E.D., (2011) 'A multi-level relational risk assessment model for secure e-government projects', *Applied Technology Integration in Governmental Organizations: New E-Government Research* (pp. 153-181). New York: IGI Global.
6. Κεφαλληνός, Δ. και Συκάς, Ε. (2011) «Μοντέλο υποδομής δημοσίου κλειδιού που προστατεύει το ιδιοαπόρρητο και την ελευθερία βούλησης», ΔΠΜΣ, Ε.Μ.Π.
7. Kefallinos, D. and Sykas, E.D., (2012) 'A personal information privacy defending public key infrastructure for the general public' (submitted to Elsevier GIQ, Manuscript #GIQ-S-12-00128)

Η σελίδα αυτή είναι σκόπιμα λευκή

ΑΚΡΩΝΥΜΑ

AHP	Analytical Hierarchy Process
BBN	Bayesian Belief Network
EG	Electronic Governance
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
ICT	Information and Communication Technology
RIPC[4]	Risk-Impact-Probabilty-CSF-Countermeasures-Cost-Coverage
ΑΔ	Αξιολόγηση Διακινδύνευσης
ΑΔΑΕ	Αρχή Διασφάλισης Απορρήτου Επικοινωνιών
ΑΔΑΠ	Ασφαλής Διάταξη Αποθήκευσης Πιστοποιητικών
ΑΕ	Αρχή Εγγραφής
ΑΕκ	Ανώνυμος Εκδότης
ΑΕξ	Αρχή Εξουσιοδότησης
ΑιΠΧ	Αίτηση Πιστοποιητικού Χαρακτηριστικών
ΑΠ	Αρχή Πιστοποίησης
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΑΠΧ	Αρχή Πιστοποιητικών Χαρακτηριστικών
ΒΔΑ	Βασικοί Δείκτες Απόδοσης
ΒΔΣ	Βασικοί Δείκτες Στόχων
ΔΤΠ	Διοίκηση Τεχνολογίας της Πληροφορίας
ΕΓ	Εντεταλμένο Γραφείο
ΕΟΑ	Ειδικό για τον Οργανισμό Αναγνωριστικό
ΕΠΕ	Εφαρμογή Πλευράς Εξυπηρετητή
ΕΠΧ	Εφαρμογή Πλευράς Χρήστη
ΕΤΑ	Έμπιστη Τρίτη Αρχή
ΗΔ	Ηλεκτρονική Διακυβέρνηση
ΚΑΠ	Κατάλογος Ανακληθέντων Πιστοποιητικών
ΚΑΤ	Καθολικό Αναγνωριστικό Ταυτοποίησης
κΕΟΑ	Κρυπτογραφημένο Ειδικό για τον Οργανισμό Αναγνωριστικό
κΜΑΑ	Κρυπτογραφημένο Μοναδικό Αδειοδοτικό Ασφαλείας
ΚΟΑ	Κωδικός Οργανισμού Αποδέκτη

ΚΠΕ	Κρίσιμοι Παράγοντες Επιτυχίας
ΜΑΑ	Μοναδικό Αδειοδοτικό Ασφαλείας
ΜΚΑ	Μοναδικό Καθολικό Αναγνωριστικό
ΟΑ	Οργανισμός Αποδέκτης
ΠΤ	Πιστοποιητικό Ταυτότητας
ΠΥΠ	Πάροχος Υπηρεσιών Πιστοποίησης
ΠΧ	Πιστοποιητικό Χαρακτηριστικών
ΤΕ	Τυφλός Εκδότης
ΤΠΕ	Τεχνολογία Πληροφορικής και Επικοινωνιών
υΑΠΧ	υπο-Αρχή Πιστοποιητικών Χαρακτηριστικών
ΥΔΚ	Υποδομή Δημοσίου Κλειδιού
ΥΔΠ	Υποδομή Διαχείρισης Προνομίων

ΜΕΤΑΦΡΑΣΗ ΟΡΟΛΟΓΙΑΣ

Αδειοδότηση ή εξουσιοδότηση πρόσβασης	Authorization
Αδειοδοτικό	Token
Αδυναμία	Weakness
Αίτηση Πιστοποιητικού (ΑιΠ)	Certificate Request (CR)
Αιτιακός λογισμός	Causal reasoning
Ακεραιότητα	Integrity
Ακολουθία πλήρωσης	Padding
Αλατισμένος μονόδρομος κατατεμαχισμός	Salted one-way hash
Αλληλεξάρτηση	Dependency
Αναγνώριση διείσδυσης	Intrusion detection
Αναγνώριση και αναχαίτιση διεισδύσεων	Intrusion detection and prevention
Ανάλυση αιτίας-αιτιατού	Cause-consequence analysis
Ανάλυση αστοχίας	Failure analysis
Ανάλυση εμποδίων	Hazard analysis
Ανάλυση κρισιμότητας	Criticality analysis
Αντίμετρο	Countermeasure
Ανώνυμη εγγραφή	Anonymous registration
Ανώνυμο αναγνωριστικό	Anonymous identifier
Ανώνυμος Εκδότης (ΑΕκ)	Anonymous Issuer (AI)
Αξιολόγηση Διακινδύνευσης (ΑΔ)	Risk Assessment, Risk Analysis (RA)
Απειλή	Threat
Απόδειξη μηδενικής γνώσης	Zero-knowledge proof
Αποκήρυξη ευθύνης	Repudiation of liability
Απόρρητο	Privacy
Αποφυγή αποκήρυξης ευθύνης	Non-repudation
Απώλεια κυριότητας	Loss of control
Αρχή Εγγραφής (ΑΕ)	Registration Authority (RA)
Αρχή Εξουσιοδότησης (ΑΕξ)	Authorization Authority (AA)
Αρχή Πιστοποίησης (ΑΠ)	Certificate Authority (CA)
Αρχή πιστοποιητικών χαρακτηριστικών	Attribute certificate authority
Ασύμμετρη κρυπτογράφηση	Asymmetric encryption
Αυτοεπαληθεύσιμο	Self-verifiable

Αυτοματοποιημένη βασισμένη σε πολιτικές αντίδραση	Policy-based automated threat response
Αυτοϋπογραφόμενο	Self-signed
Αφανής εμπιστοσύνη	Implicit trust
Βαθμός διακινδύνευσης	Risk grade
Βηματική	Stepwise
Βηματοδότηση	Pacing
Βοήθεια βάση συγκειμένου	Context sensitive help
Γένειο	Generic
Γνωσιακή βάση	Knowledge base
Γράφος επίθεσης	Attack graph
Δέντρο γεγονότων	Event tree
Δέντρο κατατεμαχισμού	Hashing tree
Δέντρο σφάλματος	Fault tree
Δημόσιο κλειδί	Public key
Διάδραση	Interaction
Διαδραστικός	Interactive
Διακριτός λογάριθμος	Discrete logarithm
Διαλειτουργικότητα	Interoperability
Διαπιστευτήριο	Credential
Διαπροσωπεία	Interface
Διεπαφή	Interface
Δίκαιη τυφλή υπογραφή	Fair blind signature
Διομότιμο	Peer-to-peer
Διπλή υπογραφή	Dual signature
Δομοστοιχείο	Module
Δομοστοιχειωτή δομή	Modular structure
Δυαδική Μεταβλητή	Binary Variable
Εκτίμηση κάλυψης	Coverage estimate
Εκτίμηση κινδύνου	Risk assessment, Risk analysis
Εκτίμηση τρωτοτήτων	Vulnerability assessment
Ελεγκτής	Verifier
Ελκωθητική	Push-pull
Εμμονή	Persistence

Εμπιστευτικότητα	Confidentiality
Έμπιστη Τρίτη Αρχή (ΕΤΑ)	Trusted Third Party (TTP)
Εμπιστοσύνη στη ρίζα	Trust-the-root
Εμφανής υπόθεση μονοτονικότητας	Explicit assumption of monotonicity
Ενδεχόμενο	Likelihood
Εντεταλμένο Γραφείο (ΕΓ)	Commissioned Office (CO)
Εξάρτηση	Dependency
Εξόρυξη δεδομένων	Data mining
Έξυπνη κάρτα	Smart card
Επαναλήπτης	Repeater
Επιγραμμικός	On-line
Επικύρωση	Validation
Επιλεκτική αποκάλυψη	Selective disclosure
Επίπεδο διακινδύνευσης	Risk level
Επίπτωση	Impact, Consequence
Επιχειρηματική περίπτωση	Business case
Επιχειρηματική συνέχεια	Business continuity
Εσφαλμένο αρνητικό	False negative
Εσφαλμένο θετικό	False positive
Εφαρμογή Πλευράς Εξυπηρετητή (ΕΠΕ)	Server-Side Application (SSA)
Εφαρμογή Πλευράς Χρήστη (ΕΠΧ)	User-Side Application (USA)
Ηλεκτρονική Διακυβέρνηση (ΗΔ)	Electronic Governance (EG)
Ιδιοαπόρρητο	Personal privacy
Ιδιωτικό κλειδί	Private key
Ιχνηλασιμότητα	Traceability
Ιχνηλάτηση	Tracing
Ιχνηλάτιση	Tracing
Κατάλογος Ανακληθέντων Πιστοποιητικών (ΚΑΠ)	Certificate Revocation List (CRL)
Κατατεμαχισμός	Hashing
Κατατομοποίηση, δημιουργία κατατομών	Profiling
Κατευθυντικός ακυκλικός γράφος	Directed acyclic graph
Κατώφλι κάλυψης	Coverage threshold
Κλιμακοθεσιμότητα	Scalability
Κυκλική κρυπτογράφηση	Circular encryption

Μετέπειτα πιθανότητα	Posterior probability
Μεσεγγύηση κλειδιού	Key escrow
Μοναδικό Καθολικό Αναγνωριστικό (ΜΚΑ)	Globally Unique Identifier (GUID)
Μονοπάτι κινδύνου	Risk path
Μονοτονικότητα	Monotonicity
Ολιστικό	Holistic
Ομόρια	Adjacency
Οπτικοποίηση	Visualization
Οργανισμός Αποδέκτης (ΟΑ)	Receiving Organization (RO)
Παραλλαγοδόρηση	Versioning
Πάροχος Υπηρεσιών Διαδικτύου (ΠΥΔ)	Internet Service Provider (ISP)
Πάροχος Υπηρεσιών Κορμού (ΠΥΚ)	Service Carrier (SC)
Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ)	Certification Service Provider (CSP)
Πιθανότητα υπό συνθήκη	Conditional Probability
Πιθανότητα	Probability
Πιστοποιητικό δημοσίου κλειδιού	Public Key Certificate (PKC)
Πιστοποιητικό Εξουσιοδότησης (ΠΕξ)	Authorization Certificate (AC)
Πιστοποιητικό μονής παρουσίασης	One-show certificate
Πιστοποιητικό πολλαπλής παρουσίασης	Multi-show certificate
Πιστοποιητικό Ταυτότητας (ΠΤ)	Identity Certificate (IdC)
Πιστοποιητικό χαμελαίων	Chameleon certificate
Πιστοποιητικό Χαρακτηριστικών (ΠΧ)	Attribute Certificate (AC)
Πληρούμενο	Padded
Πολυδένδρο	Polytree
Πολυ-παρουσιάσιμο	Multi-show
Πολυπολιτισμικότητα	Multiculturalism
Προετοιμασία απρόοπτου	Contingency planning
Πρόκληση-απάντηση	Challenge-response
Προσβλητότητα	Vulnerability
Προσιτότητα	Accessibility
Προσωπικό απόρρητο	Personal privacy
Πρότερη πιθανότητα	Prior probability
Ρητή εμπιστοσύνη	Explicit trust
Στατιστική λήψη αποφάσεων	Statistical decision theory

Συγκεχυμένος γνωσιακός χάρτης	Fuzzy cognitive map
Συμβολικός ελεγκτής	Symbolic checker
Συμβολοσειρά πρόκλησης	Challenge phrase
Συμμετρική κρυπτογράφηση	Symmetrical encryption
Συμπερασματική λογική	Deductive logic
Συνάρτηση ιεράρχησης	Hierarchy function
Συνάρτηση κατατεμαχισμού	Hashing function
Συνδεσιμότητα	Linkability
Συνεδρία	Session
Συνένωση	Concatenation
Σχεδιότυπο	Template
Ταυτοποίηση (ή επαλήθευση ταυτότητας)	Authentication
Τεχνολογία Πληροφορικής και Επικοινωνιών (ΤΠΕ)	Information & Communication Technology
Τρωτότητα	Vulnerability
Τυφλή υπογραφή	Blind signature
Τυφλός Εκδότης (ΤΕ)	Blind Issuer (BI)
Υπαναχώρηση	Backtracking
Υπάρχοντα	Assets
Υπηρεσία ιστοχώρου	Web service
Υπο-Αρχή πιστοποιητικών χαρακτηριστικών	Attribute certificate sub-Authority
Υποδομή Δημοσίου Κλειδιού (ΥΔΚ)	Public Key Infrastructure (PKI)
Υποδομή Διαχείρισης Προνομίων (ΥΔΠ)	Privilege Management Infrastructure (PMI)
Υποτελές πιστοποιητικό	Slave certificate
Φυλλομετρητής (ή διαφυλλιστής) ιστοσελίδων	Web browser
Ψευδώνυμο	Pseudonym

Η σελίδα αυτή είναι σκόπιμα λευκή

ΑΝΑΦΟΡΕΣ

Acosta, C., & Siu, N. (1993). Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. *Reliability Engineering and System Safety, 41*, 135-154.

Adar, E. (2002). *End-to-End Security Assessment.* Paper presented at the Analysis & Assessment for Critical Infrastructure Protection, Brussels.

Ammann, P., Wijesekera, D., & Kaushik, S. (2002). *Scalable, graph-based network vulnerability analysis.* Paper presented at the 9th ACM Conference on Computer and Communications Security.

Anand, P. (1993). *Foundations of Rational Choice Under Risk*: Oxford University Press.

Andrews, J. D., & Moss, T. R. (1993). *Reliability and Risk Assessment* (1st Ed. ed.): Longman Group UK.

Aven, T. (1992). *Reliability and Risk Analysis* (1st Ed. ed.): Elsevier Applied Science.

Bell, D., Cox, L., Jackson, S., & Schaefer, P. (1992). *Using Causal Reasoning for Automated Failure & Effects Analysis (FMEA).* Paper presented at the Annual Reliability and Maintainability Symposium.

Boehm, B. W. (1991). Software risk management: principles and practices. *IEEE Software, 8*, 32-41.

Bouti, A., & Kadi, D. A. (1994). A state-of-the-art review of FMEA/FMECA. *International Journal of Reliability, Quality and Safety Engineering, 1*(4), 515-543.

Brands, S. (1999). *Rethinking public key infrastructures and digital certificates - Building in Privacy.* Eindhoven Institute of Technology, Eindhoven.

Carter, B., Hancock, T., Morin, J. M., & Robins, M. (2001). *Introducing Riskman Methodology – The European Project Risk Management Methodology*. Oxford: NCC Blackwell Ltd.

Chapman, R. J. (1998). The effectiveness of working group risk identification and assessment techniques. *International Journal of Project Management, 16*(6), 333-343.

CNSS. (2003). *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*. Retrieved from http://csrc.nist.gov/groups/STM/cmvp/documents/CNSS15FS.pdf.

Cojazzi, G., & Cacciabue, P. C. (1994). *The DYLAM Approach for the Reliability Analysis of Dynamic System*. Berlin Heidelberg: Springer-Verlag.

Curthoys, N., & Crabtree, J. (2003). SmartGov: Renewing Electronic Government for Improved Service Delivery, ISociety Report Retrieved from http://www.pwc.com/uk/eng/about/ind/gov/smargovfinal.pdf

Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1975). *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*. Glenview, Illinois: Scott, Foresman and Company.

Durham, C. C. (2002). *Implementing Electronic Government Statement*. Retrieved from http://www.durham.gov.uk/.

Durofee, A. J., Walker, J. A., Alberts, C. J., Higuera, R. P., Murphy, R. L., & Williams, R. J. (1996). *Continuous Risk Management Guidebook*. Pittsburg, PA: Carnegie Mellon University.

Ebrahim, Z., & Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal, 11*(5), 589-611.

Elieson, B. D. (2006). Construction of an IT Risk Framework Retrieved from http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=33595

Evangelidis, A. (2007). FRAMES – A Risk Assessment Framework for e-Services. *Electronic Journal of e-Government, 2*(1), 21-30.

Evangelidis, A., Akomode, J., Taleb-Bendiab, A., & Taylor, M. (2002). *Risk Assessment & Success Factors for e-Government in a UK Establishment.* Paper presented at the Electronic Government, First International Conference, Aix-en-Provence France.

Fairley, R. (1994). Risk management for software projects. *IEEE Software*, 57-64.

Gil-Garcia, J. R., & Pardo, T. A. (2005). E-government success factors: mapping practical tools to theoretical foundations. *Government Information Quarterly, 22*, 187-216.

Gritzalis, D., & Katsikas, S. (2004). *Autonomy and political disobedience in cyberspace*. Athens: Papasotiriou.

Hampshire, C. C. (2006). *Section 5: Risk Assessment*. Retrieved from http://www.hants.gov.uk/egovernment/IEG2-sec5.html.

Hansson, S. O. (1994). Decision Theory, A Brief Introduction Retrieved from http://www.infra.kth.se/~soh/decisiontheory.pdf

ISO/IEC. (2004). Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions, ISO/IEC 10118-3:2004: International Organization for Standardization.

ISO/IEC. (2005a). 27001:2005 Information security management systems - Requirements *Current Stage 90.92* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

ISO/IEC. (2005b). 27002:2005 Code of practice for information security management *Current Stage 90.92* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297

ISO/IEC. (2008). 27005:2008 Information security risk management *Current Stage 90.92* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107

ISO/IEC. (2009). 27004:2009 Information security management -- Measurement *Current Stage 60.60* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42106

ISO/IEC. (2010). 27003:2010 Information security management system implementation guidance *Current Stage 60.60* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42105

ITU-T. (2005). Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

ITU-T. (2008). Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks.

Jaeger, P. T. (2003). The endless wire: E-government as global phenomenon. *Government Information Quarterly 20*, 323-331.

Jha, S., Sheyner, O., & Wing, J. M. (2002, June 24-26). *Two formal analyses of attack graphs.* Paper presented at the 15th IEEE Computer Security Foundations Workshop, Nova Scotia, Canada.

Jouko, S., & Rouhiainen, V. (1993). *Quality Management of Safety and Risk Analysis*: Elsevier Science Publishers B.V.

Kara-Zaitri, C., Keller, A. Z., Barody, I., & Fleming, P. V. (1991). *An Improved FMEA methodology.* Paper presented at the Annual Reliability and Maintainability Symposium.

Kara-Zaitri, C., Keller, A. Z., & Fleming, P. V. (1992). *A Smart Failure Mode and Effect Analysis Package.* Paper presented at the Annual Reliability and Maintainability Symposium.

Kefallinos, D., Lambrou, M. A., & Sykas, E. D. (2009). An Extended Risk Assessment Model for Secure E-Government Projects. *International Journal of Electronic Government Research, 5*(2), 72-92.

Kefallinos, D., Lambrou, M. A., & Sykas, E. D. (2011). A multi-level relational risk assessment model for secure e-government projects *Applied Technology Integration in Governmental Organizations: New E-Government Research* (pp. 153-181). New York: IGI Global.

Kefallinos, D., Lamprou, M. A., & Sykas, E. D. (2006). Secure PKI-enabled E-Government Infrastructures Implementation: the SYZEFXIS-PKI Case. *Electronic Government International Journal, 3*(4), 420-438.

Kefallinos, D., & Sykas, E. D. (2012). A personal information privacy defending public key infrastructure for the general public. *Government Information Quarterly*.

Klein, J. H., & Cork, R. B. (1998). An approach to technical risk assessment. *International Journal of Project Management, 16*(6), 345-351.

Knox, N. W., & Eicher, R. W. (1992). MORT User' s Manual, rev. 3: US Department of Energy, System Safety Development Center EG&G Idaho Inc.

Lim, E. T. K., Tan, C. H., & Pan, S. L. (2007). E-Government Implementation: Balancing Collaboration and Control in Stakeholder Management. *International Journal of Electronic Government Research, 3*(2), 1-28.

Löfstedt, U. (2005). E-Government – Assessment of Current Research and Proposals for Future Directions Retrieved from http://www.hia.no/iris28/Docs/IRIS2028-1008.pdf

Martin, N. (2005). Why Australia needs a SAGE: a security architecture for the Australian government environment. *Government Information Quarterly, 22*, 96-107.

NECCC. (2000). Risk Assessment Guidebook for e-Commerce/e-Government Retrieved from http://www.ec3.org/Downloads/2000/Risk_Assessment_Guidebook.pdf

NIST. (2001). *Advanced Encryption Standard (AES)*. Retrieved from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Noel, S., & Jajodia, S. (2004). *Managing attack graph complexity through visual hierarchical aggregation.* Paper presented at the ACM Workshop on Visualization and Data Mining for Computer Security, New York.

OECD. (2001). *The Hidden Threat to E-Government: Avoiding large government IT failures*. Retrieved from http://www.oecd.org/dataoecd/19/12/1901677.pdf.

Ou, X., Boyer, F. W., & McQueen, M. A. (2006, October 30-November 3). *A Scalable Approach to Attack Graph Generation.* Paper presented at the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA.

Pate-Cornell, M. E. (1984). Fault Tree vs. Event Trees in Reliability Analysis. *Risk Analysis, 4*(3), 177-186.

Pate-Cornell, M. E. (1993). Risk Analysis and Risk Management for Offshore Platforms: Lessons from the Piper Alpha Accident. *Journal of Offshore Mechanics and Arctic Engineering, 115*, 179-190.

Pelaez, C. E., & Bowles, J. B. (1995). *Applying Fuzzy Cognitive-Maps Knowledge-Representation to Failure Modes Effects Analysis.* Paper presented at the Annual Reliability and Maintainability Symposium.

Phillips, C. A., & Swiler, L. P. (1998, September 22-25). *A graph-based system for network-vulnerability analysis.* Paper presented at the Workshop on New Security Paradigms, Charlottsville, VA, USA.

Press, S. J. (1989). *Bayesian Statistics: Principles, Models and Applications*. New York, NY: Wiley.

Price, C. J., Hunt, J. E., Lee, M. H., & Ormsby, R. T. (1992). A Model-based Approach to the Automation of Failure Mode Effects Analysis for Design. *IMechE, Part D: the Journal of Automobile Engineering, 206*, 285-291.

Relyea, H. C. (2002). E-gov: Introduction and overview. *Government Information Quarterly, 19*(1), 9-35.

Rieke, R. (2004). *Tool based formal modelling, analysis and visualisation of enterprise network vulnerabilities utilising attack graph exploration.* Paper presented at the EICAR 2004 Conference, Copehagen.

Ritchey, R., & Ammann, P. (2001, May). *Using model checking to analyze network vulnerabilities.* Paper presented at the IEEE Symposium on Security and Privacy.

Roy, J. (2003). E-government. *Social Science Computer Review, 21*(1), 3-5.

Saaty, T. L. (2001). *Decision Making for Leaders – The Analytical Hierarchy Process for Decisions in a Complex World*. Pittsburgh, PA: RWS Publications.

Schmidt, R. C., Lyytinen, K., Keil, M., & P. Cule, P. (2001). Identifying software project risks: an international Delphi study. *Journal of Management Information Systems, 17*(4), 5-36.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1998). Twofish: A 128-Bit Block Cipher. Retrieved from http://www.schneier.com/paper-twofish-paper.html

Sheyner, O., Haines, J. W., Jha, S., Lippmann, R., & Wing, J. M. (2002, May). *Automated generation and analysis of attack graphs.* Paper presented at the IEEE Symposium on Security and Privacy, Oakland, California.

Siu, N. (1994). Risk Assessment for dynamic systems: An overview. *Reliability Engineering and System Safety, 43*, 43-73.

Snellen, I. (2002). Electronic governance: Implications for citizens, politicians and public servants. *International Review of Administrative Sciences, 68*(2), 183-198.

Stamatis, D. H. (1995). *Failure Mode and Effect Analysis - FMEA from Theory to Execution*: ASQC Quality Press.

Sutton, I. S. (1992). *Process Reliability and Risk Management* (1st Ed. ed.): Van Nostrand Reinhold.

Swiler, L. P., Phillips, C., Ellis, D., & Chakerian, S. (2001, June 12-14). *Computer-attack graph generation tool.* Paper presented at the DARPA Information Survivability Conference and Exposition, Anaheim, California.

Tan, C. W., Pan, S. L., & Lim, E. T. K. (2007). Managing Stakeholder Interests in E-Government Implementation: Lessons Learned from a Singapore E-Government Project. *International Journal of Electronic Government Research, 3*(1), 61-84.

Tasmania. (2005). Risk Management Resource Kit. from http://www.egovernment.tas.gov.au/themes/project_management/risk_management_resource_kit

Titah, R., & Barki, H. (2006). E-Government Adoption and Acceptance: A Literature Review. *International Journal of Electronic Government Research, 2*(3), 23-57.

Tseng, M. M., Kyellberg, T., & Lu, S. C. Y. (2003). Design in the new e-manufacturing era. *Annals of the CIRP, 52*(2).

Vassilakis, C., Lepouras, G., Fraser, J., & Georgiadis, P. (2005). Barriers To Electronic Service Development. *e-Service Journal, 4*(1), 41-63.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.