

ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ
ΑΝΑΛΥΤΙΚΟ ΥΠΟΜΝΗΜΑ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΕΡΓΑΣΙΩΝ

Δρ. ΤΣΩΧΟΥ ΑΓΓΕΛΙΚΗ

Επίκουρος Καθηγήτρια σε

Ιδιωτικότητα και Ασφάλεια Πληροφοριακών Συστημάτων

Τμήμα Πληροφορικής

Ιόνιο Πανεπιστήμιο

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ	1
A. ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ	3
A.1 ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ	3
A.2 ΣΠΟΥΔΕΣ	3
A.3 ΕΡΕΥΝΗΤΙΚΑ ΕΝΔΙΑΦΕΡΟΝΤΑ	3
A.4 ΠΑΡΟΥΣΑ ΑΠΑΣΧΟΛΗΣΗ	4
A.5 ΣΥΝΟΨΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΕΜΠΕΙΡΙΑΣ	4
A.6 ΔΙΑΚΡΙΣΕΙΣ	4
A.7 ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ	5
A.7.1 ΔΙΔΑΚΤΙΚΗ ΕΜΠΕΙΡΙΑ	5
A.7.2 ΕΠΙΒΛΕΨΗ ΥΠΟΨΗΦΙΩΝ ΔΙΔΑΚΤΟΡΩΝ ΚΑΙ ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΞΕΤΑΣΤΙΚΕΣ ΕΠΙΤΡΟΠΕΣ ΔΙΔΑΚΤΟΡΙΚΩΝ ΔΙΑΤΡΙΒΩΝ	7
A.7.3 ΕΠΙΒΛΕΨΗ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΔΙΠΛΩΜΑΤΙΚΩΝ ΕΡΓΑΣΙΩΝ	7
A.7.4 ΕΠΙΒΛΕΨΗ ΠΤΥΧΙΑΚΩΝ ΕΡΓΑΣΙΩΝ	8
A.7.3 ΕΡΕΥΝΗΤΙΚΗ ΕΜΠΕΙΡΙΑ - ΕΡΓΑ ΕΡΕΥΝΑΣ	8
A.7.4 ΛΟΙΠΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ	10
A.8 ΔΗΜΟΣΙΕΥΜΕΝΟ ΕΡΓΟ	10
A.8.1 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ ΜΕ ΣΥΣΤΗΜΑ ΚΡΙΤΩΝ	10
A.8.2 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΠΡΑΚΤΙΚΑ ΔΙΕΘΝΩΝ ΣΥΝΕΔΡΙΩΝ ΜΕ ΚΡΙΣΗ ΠΛΗΡΟΥΣ ΚΕΙΜΕΝΟΥ	12
A.8.3 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ WORKSHOPS, POSTERS ΚΑΙ ΠΕΡΙΛΗΨΕΙΣ ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ ΜΕ ΚΡΙΣΗ	14
A.8.4 ΔΙΑΤΡΙΒΕΣ	15
A.9 ΠΡΟΣΚΕΚΛΗΜΕΝΕΣ ΟΜΙΛΙΕΣ	15
A.9.1 ΚΕΝΤΡΙΚΗ ΟΜΙΛΗΤΡΙΑ	15
A.9.2 ΟΜΙΛΗΤΡΙΑ	16
A.10 ΔΙΟΡΓΑΝΩΣΗ ΔΙΕΘΝΩΝ ΣΥΝΕΔΡΙΩΝ ΚΑΙ ΣΕΜΙΝΑΡΙΩΝ	16
A.10.1 ΔΙΟΡΓΑΝΩΣΗ ΘΕΡΙΝΩΝ ΣΧΟΛΕΙΩΝ	16
A.10.2 ΔΙΟΡΓΑΝΩΣΗ ΣΥΝΕΔΡΙΩΝ ΚΑΙ WORKSHOPS	16
A.11 ΣΥΝΤΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	16
A.11.1 ΜΕΛΟΣ ΣΥΝΤΑΚΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΠΕΡΙΟΔΙΚΩΝ	16
A.11.2 ΜΕΛΟΣ ΣΥΝΤΑΚΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΠΕΡΙΟΔΙΚΩΝ – ΕΞΕΙΔΙΚΕΥΜΕΝΑ ΤΕΥΧΗ	16
A.11.3 ΜΕΛΟΣ ΕΠΙΣΤΗΜΟΝΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΓΡΑΜΜΑΤΟΣ (PROGRAM COMMITTEE MEMBER) ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ	17

A.11.4 ΚΡΙΤΗΣ (REVIEWER) ΕΡΕΥΝΗΤΙΚΩΝ ΕΡΓΑΣΙΩΝ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ	18
A.11.5 ΠΡΟΕΔΡΕΥΟΥΣΑ ΘΕΜΑΤΙΚΗΣ ΕΝΟΤΗΤΑΣ (TRACK CHAIR) ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ	18
A.11.6 ΚΡΙΤΗΣ (REVIEWER) ΕΡΕΥΝΗΤΙΚΩΝ ΕΡΓΑΣΙΩΝ ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ	19
A.12 ΔΙΟΙΚΗΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	21
A.12.1 ΣΥΜΜΕΤΟΧΗ ΣΕ ΟΜΑΔΕΣ ΕΡΓΑΣΙΑΣ	21
B. ΑΝΑΛΥΤΙΚΟ ΥΠΟΜΝΗΜΑ ΓΙΑ ΤΙΣ ΥΠΟΒΑΛΛΟΜΕΝΕΣ ΕΠΙΣΤΗΜΟΝΙΚΕΣ ΔΗΜΟΣΙΕΥΣΕΙΣ	22
B.1 ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ	22
B.2 ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ ΔΗΜΟΣΙΕΥΜΕΝΕΣ ΣΕ ΔΙΕΘΝΗ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ	24
B.3 ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ ΔΗΜΟΣΙΕΥΜΕΝΕΣ ΣΕ ΠΡΑΚΤΙΚΑ ΔΙΕΘΝΩΝ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΣΥΝΕΔΡΙΩΝ ΜΕΤΑ ΑΠΟ ΚΡΙΣΗ ΠΛΗΡΟΥΣ ΚΕΙΜΕΝΟΥ	36

A. ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

A.1 ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ

Όνοματεπώνυμο:	Τσώχου Αγγελική
Όνόματα γονέων:	Γεώργιος και Μαρία
Ημερομηνία γέννησης:	6 Οκτωβρίου 1980
Ηλεκτρονική Διεύθυνση:	atsohou@ionio.gr
Τηλέφωνο Εργασίας:	+30 - 2261087738
Διεύθυνση Ιστοσελίδας:	http://di.ionio.gr
Google Scholar:	https://scholar.google.com/citations?user=etn5eNkAAAAJ&hl=en

A.2 ΣΠΟΥΔΕΣ

ISO 27001 Lead Auditor (2016), Information Security Management Systems (ISMS) Auditor/Lead Auditor (In accordance with ISO 27001:2013), TUV NORD, IRCA Certified Training Course

Μεταδιδακτορική Ερευνήτρια (Post-Doctoral Researcher) (2013-2014), University of Jyväskylä, Department of Computer Science and Information Systems, Φινλανδία

Μεταδιδακτορική Ερευνήτρια (Post-Doctoral Researcher) (2011-2013), Brunel University West London, Business School, Ηνωμένο Βασίλειο

Διδακτορικό Δίπλωμα (Άριστα), Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου (2010), Τίτλος διδακτορικής διατριβής: *Η Ενημερότητα Ασφάλειας στα Πλαίσια της Διοίκησης Ασφάλειας Πληροφοριακών Συστημάτων*

Μεταπτυχιακό Δίπλωμα στα *Πληροφοριακά Συστήματα* (Άριστα), Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών (2002-2004)

Πτυχίο Πληροφορικής (Λίαν Καλώς), Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών (1998-2002)

A.3 ΕΡΕΥΝΗΤΙΚΑ ΕΝΔΙΑΦΕΡΟΝΤΑ

- Πολιτικές Ασφάλειας, Αντιλήψεις Επικινδυνότητας και Ενημερότητα Χρηστών (Information Security Policies, Risk Perceptions and User Awareness)
- Ανάλυση Επικινδυνότητας και Διοίκηση Ασφάλειας Πληροφοριών (Information Security Risk Assessment and Management)
- Πολιτικές Ασφάλειας για την Ορθή Χρήση του Διαδικτύου (Security Policies for Acceptable Internet Use)
- Ιδιωτικότητα στο Διαδίκτυο και Εργαλεία Ενίσχυσης της Ιδιωτικότητας (Internet Privacy and Privacy Enhancing Tools)

- Ιδιωτικότητα σε Διαδικτυακές Εφαρμογές Κινητών Συσκευών (Privacy Protection in Mobile Applications)
- Πρότυπα Ασφάλειας και Ιδιωτικότητας (Information Security and Privacy Standards)
- Ηλεκτρονικές Υπηρεσίες Διαδικτύου, Ηλεκτρονική Διακυβέρνηση και Πληροφοριακά Συστήματα (e-Services, e-Government and Information Systems)

A.4 ΠΑΡΟΥΣΑ ΑΠΑΣΧΟΛΗΣΗ

Σεπτέμβριος 2016 - Σήμερα: Επίκουρος Καθηγήτρια σε Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο, Ιόνιο Πανεπιστήμιο, Τμήμα Πληροφορικής, Κέρκυρα, Ελλάδα

A.5 ΣΥΝΟΨΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗΣ ΕΜΠΕΙΡΙΑΣ

- A.5.1 **Σεπτέμβριος 2014 – Αύγουστος 2016: Λέκτορας** σε Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο, Ιόνιο Πανεπιστήμιο, Τμήμα Πληροφορικής, Κέρκυρα, Ελλάδα
- A.5.2 **Ιούλιος 2013 – Αύγουστος 2014:** Μεταδιδακτορική ερευνήτρια (Post-Doctoral Researcher), University of Jyväskylä, Department of Computer Science and Information Systems, Φινλανδία.
- A.5.3 **Ιούλιος 2012 - Ιούνιος 2013:** Ειδικευμένη ερευνήτρια (Senior Research Fellow) σε ασφάλεια και ιδιωτικότητα δημοσίων υπηρεσιών σε περιβάλλοντα νεφούπολογιστικής, Brunel University West London, Ηνωμένο Βασίλειο.
- A.5.4 **Ιούνιος 2011 – Ιούνιος 2012:** Ειδικευμένη ερευνήτρια (Senior Research Fellow, Marie Curie FP7 People) σε μηχανική επιχειρησιακών διαδικασιών (process engineering) σε περιβάλλοντα ηλεκτρονικής διακυβέρνησης, Brunel University West London, Ηνωμένο Βασίλειο.
- A.5.5 **Δεκέμβριος 12.2009 – Ιούνιος 2011:** Ειδική Συνεργάτης του Ειδικού Γραμματέα Επιχειρησιακού Προγράμματος «Διοικητική Μεταρρύθμιση 2007-2013» του Υπουργείου Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης, Ελλάδα
- A.5.6 **Σεπτέμβριος 2010 – Ιούλιος 2011:** Διδάσκουσα βάσει του Π.Δ. 407/80, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς, Ελλάδα
- A.5.7 **Φεβρουάριος 2010 – Ιούλιος 2010:** Επιστημονικός Συνεργάτης, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς, Ελλάδα
- A.5.8 **Μάρτιος 2005 – Σεπτέμβριος 2009:** Συμμετοχή σε ερευνητικά και αναπτυξιακά έργα μέσω των ερευνητικών ομάδων του Πανεπιστημίου Αιγαίου και του Οικονομικού Πανεπιστημίου Αθηνών, Ελλάδα

A.6 ΔΙΑΚΡΙΣΕΙΣ

- A.6.1 **Outstanding Reviewer 2013** για το επιστημονικό Περιοδικό Transforming Government: People, Process and Policy, Emerald Literati Network Awards for Excellence 2013 (http://www.emeraldinsight.com/authors/literati/reviewer_2013.htm)
- A.6.2 **Outstanding Reviewer 2012** για το επιστημονικό Περιοδικό Journal Information Management and Computer Security, Emerald Literati Network Awards for Excellence 2012 (http://www.emeraldinsight.com/authors/literati/reviewer_2012.htm)

- A.6.3 **Υποτροφία Marie Curie 2011**, στο πλαίσιο Επιστημονικού Έργου υπό χρηματοδότηση από την Ευρωπαϊκή Επιτροπή
- A.6.4 **Highly Commended Award Winner for Outstanding Paper at the Emerald Literati Network Awards for Excellence 2009** για το άρθρο Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., "Process-Variance Models in Information Security Awareness Research", *Information Management and Computer Security*, Vol.16, No. 3, pp. 271 – 287, 2008 (<http://www.emeraldinsight.com/authors/literati/awards.htm?year=2009&journal=imcs>)
- A.6.5 **Πρότυπο Άρθρο (Sample Article)** για το περιοδικό Information Management and Computer Security 2009 για το άρθρο για το άρθρο Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., "Process-Variance Models in Information Security Awareness Research", *Information Management and Computer Security*, Vol.16, No. 3, pp. 271 – 287, 2008
- A.6.6 **Υποτροφία από το Μεταπτυχιακό Πρόγραμμα Σπουδών στα Πληροφοριακά Συστήματα (Αριστα)**, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών (2002-2004)

A.7 ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ

A.7.1 ΔΙΔΑΚΤΙΚΗ ΕΜΠΕΙΡΙΑ

Μεταπτυχιακά Προγράμματα Σπουδών

- A.7.1.1 **Διδάσκουσα**, αυτοδύναμη διδασκαλία ενοτήτων στο πλαίσιο του μαθήματος *Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας στο Διαδίκτυο* (Χειμερινό εξάμηνο, 2015; Χειμερινό εξάμηνο, 2016), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Πληροφορική, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο
- A.7.1.2 **Διδάσκουσα**, αυτοδύναμη διδασκαλία ενοτήτων στο πλαίσιο του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων* (Εαρινό εξάμηνο, 2016; Εαρινό εξάμηνο 2017), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Πληροφορική, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο
- A.7.1.3 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων και Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας* (Χειμερινό Εξάμηνο, 2016), Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου
- A.7.1.4 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Πληροφοριακά Συστήματα* (Χειμερινό Εξάμηνο, 2016), Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου
- A.7.1.5 **Προσκεκλημένη Εισηγήτρια**, αυτοδύναμη διδασκαλία ενοτήτων του μαθήματος *Γλώσσες Προγραμματισμού και Βιολογικές Βάσεις Δεδομένων* (Χειμερινό εξάμηνο, 2016), Πρόγραμμα Μεταπτυχιακών Σπουδών Βιοπληροφορική και Νευροπληροφορική, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο
- A.7.1.6 **Προσκεκλημένη Εισηγήτρια**, αυτοδύναμη διδασκαλία ενοτήτων του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων και Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας* (Χειμερινό εξάμηνο, 2015), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου

- A.7.1.7 **Προσκεκλημένη Εισηγήτρια**, αυτοδύναμη διδασκαλία ενοτήτων του μαθήματος *Διοίκηση Πληροφοριακών Συστημάτων* (Εαρινό εξάμηνο, 2015), Πρόγραμμα Μεταπτυχιακών Σπουδών σε Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου
- A.7.1.8 **Διδάσκουσα βάσει του Π.Δ. 407/80**, αυτοδύναμη διδασκαλία ενοτήτων στο πλαίσιο του μαθήματος *Πολιτικές και Διαχείριση Ασφάλειας* (Εαρινό Εξάμηνο 2011), Πρόγραμμα Μεταπτυχιακών Σπουδών, Μεταπτυχιακό Δίπλωμα Ειδίκευσης «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων», Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς
- A.7.1.9 **Επιστημονικός Συνεργάτης**, διαμόρφωση και διδασκαλία της ύλης δύο διαλέξεων του μαθήματος: *Πολιτικές και Διαχείριση Ασφάλειας* (Εαρινό Εξάμηνο 2010), Πρόγραμμα Μεταπτυχιακών Σπουδών, Μεταπτυχιακό Δίπλωμα Ειδίκευσης «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων», Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς.

Προπτυχιακά Προγράμματα Σπουδών

- A.7.1.1 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Πολιτικές και Τεχνολογίες Ασφάλειας και Ιδιωτικότητας* (Ε' Εξάμηνο, 2014 - Σήμερα), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο
- A.7.1.2 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων* (Η' Εξάμηνο, 2015 - Σήμερα), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο
- A.7.1.3 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Ειδικά Θέματα Ασφάλειας Πληροφοριών* (Στ' Εξάμηνο, 2016 - Σήμερα), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο
- A.7.1.4 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Μαθηματικός Προγραμματισμός* (Ε' Εξάμηνο, 2014 - Σήμερα), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο
- A.7.1.5 **Διδάσκουσα**, αυτοδύναμη διδασκαλία του μαθήματος *Συστήματα Υποστήριξης Αποφάσεων* (Στ' Εξάμηνο, 2015), Πρόγραμμα Προπτυχιακών Σπουδών, Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο
- A.7.1.6 **Ειδικευμένη Ερευνήτρια**, Διδασκαλία στα πλαίσια μεταδιδακτορικής έρευνας, συνδιδασκαλία του μαθήματος “Information Security Management” (εαρινό εξάμηνο, 2014), σε συνεργασία με τον Καθ. Sironen Mikko, Τμήμα Επιστήμης Υπολογιστών και Πληροφοριακών Συστημάτων, University of Jyväskylä, Finland
- A.7.1.7 **Διδάσκουσα βάσει του Π.Δ. 407/80**, αυτοδύναμη διδασκαλία του μαθήματος *Πολιτικές και Διαχείριση Ασφάλειας* (χειμερινό εξάμηνο 2010) Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς.
- A.7.1.8 **Διδάσκουσα βάσει του Π.Δ. 407/80**, αυτοδύναμη διδασκαλία του μαθήματος *Ασφάλεια Πληροφοριακών Συστημάτων* (Εαρινό Εξάμηνο, 2011) Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς.
- A.7.1.9 **Επιστημονικός Συνεργάτης**, αυτοδύναμη διδασκαλία, διαμόρφωση και διδασκαλία της ύλης του μαθήματος: *Ασφάλεια Πληροφοριακών Συστημάτων* (Εαρινό Εξάμηνο 2010), Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς.

Προγράμματα Κατάρτισης και Επιμόρφωσης

- A.7.1.10 Εισηγήτρια θεμάτων ασφάλειας πληροφοριακών συστημάτων, **Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης** (2.2010-4.2010)
- A.7.1.11 Εισηγήτρια θεμάτων Προτύπων Ασφάλειας Πληροφοριακών Συστημάτων και θεμάτων Επιχειρησιακής Συνέχειας στο **European Intensive Programme on Information and Communication Technologies Security** (IPICS 2009, 2010, 2011, 2012, 2013)

A.7.2 ΕΠΙΒΛΕΨΗ ΥΠΟΨΗΦΙΩΝ ΔΙΔΑΚΤΟΡΩΝ ΚΑΙ ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΞΕΤΑΣΤΙΚΕΣ ΕΠΙΤΡΟΠΕΣ ΔΙΔΑΚΤΟΡΙΚΩΝ ΔΙΑΤΡΙΒΩΝ

- A.7.2.1 **Επιβλέπουσα** διδακτορικής διατριβής του Ιωάννη Πασπάτη, «Από-ανωνυμοποίηση δεδομένων εφαρμογών κινητών τηλεφώνων και κίνδυνοι ιδιωτικότητας», Ιόνιο Πανεπιστήμιο, σε εξέλιξη
- A.7.2.2 Μέλος της Τριμελούς Επιτροπής της διδακτορικής διατριβής του Ανδρέα Σκάλκου, «Πληροφοριακή Ιδιωτικότητα και Ανθρώπινη Συμπεριφορά», Πανεπιστήμιο Αιγαίου, σε εξέλιξη
- A.7.2.3 **Εξωτερική κριτής** διδακτορικής διατριβής του *Jouko Selkälä*, για τη διδακτορική διατριβή με τίτλο “Chief Information Officer decision making: Issues and a Process View”, Department of Computer Science and Information Systems, University of Jyväskylä, Νοέμβριος 2015.
- A.7.2.4 Μέλος της Επταμελούς Εξεταστικής Επιτροπής της διδακτορικής διατριβής του Σίμου Σταύρου με τίτλο Designing Cloud Forensic-Enabled System, Πανεπιστήμιο Αιγαίου, Ιούνιο 2017
- A.7.2.5 **Εξωτερική κριτής** διδακτορικής διατριβής της *Ana Nieto Jiménez*, για τη διδακτορική διατριβή με τίτλο “Design of Mechanisms for Development of Secure Systems trading-off Quality of Service”, University of Malaga, Μάιος 2015.
- A.7.2.6 **Εξωτερική Κριτής** της διδακτορικής διατριβής του *Jouko Selkälä* με τίτλο «Chief Information Officer Decision making: Issues and a Process View, Πανεπιστήμιο της Jyväskylä, Νοέμβριος 2015.

A.7.3 ΕΠΙΒΛΕΨΗ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΔΙΠΛΩΜΑΤΙΚΩΝ ΕΡΓΑΣΙΩΝ

- A.7.3.1 **Επιβλέπουσα** στη μεταπτυχιακή διπλωματική εργασία της Κατερίνας Σουμελίδου με τίτλο Privacy Policy Visualization and Information Privacy Awareness, Ιόνιο Πανεπιστήμιο, Ιούλιος 2017
- A.7.3.2 **Επιβλέπουσα** στη μεταπτυχιακή διπλωματική εργασία του Θάνου Παπαϊωάννου με τίτλο Η διαμόρφωση της Ψηφιακής Ταυτότητας και η Αντίληψη της Ιδιωτικότητας στα Μέσα Κοινωνικής Δικτύωσης, Ιόνιο Πανεπιστήμιο, Ιούλιος 2017
- A.7.3.3 **Επιβλέπουσα** στη μεταπτυχιακή διπλωματική εργασία της Αγγελικής Παγκράτη, Συνεργατική μάθηση με υποστήριξη υπολογιστή (CSCL): Ανάπτυξη εκπαιδευτικού υλικού σε σύγχρονα περιβάλλοντα μάθησης σχετικά με την ασφάλεια στο διαδίκτυο, Ιόνιο Πανεπιστήμιο, σε εξέλιξη
- A.7.3.4 **Επιβλέπουσα** στη μεταπτυχιακή διπλωματική εργασία του Ιωάννη Κουριπά, Επαγρύπνηση μαθητών Πρωτοβάθμιας εκπαίδευσης περί Ιδιωτικότητας στο Διαδίκτυο, Ιόνιο Πανεπιστήμιο, σε εξέλιξη

- A.7.3.5 **Συνεπιβλέπουσα** στη μεταπτυχιακή διπλωματική εργασία του Ιωάννη Πασπάτη, Ενημερότητα ιδιωτικότητας σε εφαρμογές κινητών συσκευών μέσω τεχνικών οπτικοποίησης, Πανεπιστήμιο Αιγαίου, Φεβρουάριος 2017
- A.7.3.6 **Μέλος της εξεταστικής επιτροπής** στη μεταπτυχιακή διπλωματική εργασία του Γεωργίου Φελούκα, Information Security Policies for Critical Infrastructures, Ιόνιο Πανεπιστήμιο, Ιούλιος 2017
- A.7.3.7 **Μέλος της εξεταστικής επιτροπής** στη μεταπτυχιακή διπλωματική εργασία του Άγγελου Προβατά, Privacy Enhancing Tools and Forensics Investigation, Ιόνιο Πανεπιστήμιο, Ιούλιος 2017

A.7.4 ΕΠΙΒΛΕΨΗ ΠΤΥΧΙΑΚΩΝ ΕΡΓΑΣΙΩΝ

- A.7.3.8 **Επιβλέπουσα** στη πτυχιακή εργασία της Εμμανουέλας Ορφανου, Οι Καθοριστικοί Παράγοντες των Αντιλήψεων Ιδιωτικότητας των Ελλήνων Χρηστών Κοινωνικών Δικτύων και η Επίδρασή τους στην Υιοθέτηση Προστατευτικής Συμπεριφοράς, Ιόνιο Πανεπιστήμιο, σε εξέλιξη
- A.7.4.1 **Επιβλέπουσα** στη πτυχιακή εργασία του Ιωάννη Παλλή, Αξιολόγηση Εργαλείων Ενίσχυσης της Διαφάνειας και Ιδιωτικότητας, Ιόνιο Πανεπιστήμιο, Ιούνιος 2016
- A.7.4.2 **Επιβλέπουσα** στη πτυχιακή εργασία της Μαγδαληνής Ορφανού, Προστασία προσωπικών δεδομένων και αντίληψη ιδιωτικότητας εργαζομένων στο πλαίσιο εταιρειών τραπεζικής, Ιόνιο Πανεπιστήμιο, Μάιος 2016

A.7.3 ΕΡΕΥΝΗΤΙΚΗ ΕΜΠΕΙΡΙΑ - ΕΡΓΑ ΕΡΕΥΝΑΣ

Διεθνή Ερευνητικά Έργα

- A.7.3.1 **Εξειδικευμένος Σύμβουλος σε Ενημερότητα Ασφάλειας Πληροφοριών**, Expert Services related to the European Cyber Security Month (ECSM) in 2017, ENISA (11.2016-08.2017)
- A.7.3.2 **Process Engineer**, EU Programme FP7/Marie Curie People Project Reference IAPP-2008-230658: “CEES - Citizen oriented Evaluation of E-Government Systems”, Brunel University, (07.2011-04.2013).
- A.7.3.3 **Information Systems Evaluation**, EU Programme FP7/Project Reference INFISO-ICT-248010: “UbiPOL- Ubiquitous Participation Platform for Policy Making”, Brunel University, (08.2011-04.2013).
- A.7.3.4 **Information Privacy Manager**, EU Programme FP7/Project Reference CIP-ICT-PSP-2011-5: “Openly Accessible Services and Interacting Society”, Brunel University, (02.2012-06.2013).

Μελετητικά και Αναπτυξιακά Έργα Εθνικής Εμβέλειας

- A.7.3.5 **Αναλύτρια Επικινδυνότητας**, Έργο “Εκπαίδευση Λειτουργών Α' Τμήμα Υπηρεσιών Πληροφορικής - Πρότυπο 904 Διαχείριση Κινδύνων”, PLANET A.E., 2016.
- A.7.3.6 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Ασφάλειας για τα Γεωγραφικά Συστήματα Πληροφοριών (Ηλεκτρονική Πολεοδομία) για τις Νομαρχιακές Αυτοδιοικήσεις της Χώρας”, TREK Consulting - Πανεπιστήμιο Αιγαίου, 2009.

- A.7.3.7 **Ερευνήτρια**, «Παραγωγή εκπαιδευτικού υλικού με θεματική ενότητα “ασφάλεια πληροφοριακών συστημάτων σε περιβάλλοντα ηλεκτρονικής διακυβέρνησης” για το έργο κατάρτιση και πιστοποίηση σε βασικές δεξιότητες και κατάρτιση σε προηγμένες δεξιότητες στη χρήση ΤΠΕ εργαζομένων στην τοπική αυτοδιοίκηση», PLANET A.E., 2009.
- A.7.3.8 **Αναλύτρια Επικινδυνότητας**, Έργο «Μελέτη Ασφάλειας για το Ολοκληρωμένο Πληροφοριακό Σύστημα και τη Διαδικτυακή Πύλη επικοινωνίας του Εθνικού Παρατηρητηρίου για τις ΜΜΕ», TREK Consulting - EOMMEX - Πανεπιστήμιο Αιγαίου, 2008-09.
- A.7.3.9 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Ασφάλειας των Ολοκληρωμένων Πληροφοριακών Συστημάτων και εγκαταστάσεων για τις υποστηρικτικές λειτουργίες των Νομαρχιακών Αυτοδιοικήσεων”, ΕΠΙΣΕΥ/ΕΜΠ - Πανεπιστήμιο Αιγαίου, (11.2007 – 04.2008).
- A.7.3.10 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Ασφάλειας του Πληροφοριακού Συστήματος Λειτουργικής Περιοχή Βιομηχανίας και Ορυκτού Πλούτου των Νομαρχιακών Αυτοδιοικήσεων και εγκαταστάσεων των Νομαρχιακών Αυτοδιοικήσεων”, KANTOR AE - Πανεπιστήμιο Αιγαίου, (04.2008 – 07.2008)
- A.7.3.11 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Ασφάλειας του Πληροφοριακού Συστήματος Ενημέρωσης και Εξυπηρέτησης Συνταξιούχων της Γενικής Γραμματείας Πληροφοριακών Συστημάτων”, Quality and Reliability A.E. - INTRACOM – Πανεπιστήμιο Αιγαίου, (11.2007-02.2008).
- A.7.3.12 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Αποτίμησης Επικινδυνότητας & Σχεδίου Ασφαλείας της Κεντρικής Κυβερνητικής Διαδικτυακής Πύλης της Δημόσιας Διοίκησης για την Πληροφόρηση & Ασφαλή Διεκπεραίωση Ηλεκτρονικών Συναλλαγών των Πολιτών/Επιχειρήσεων”, Info-Quest - Decision Systems Integration – Πανεπιστήμιο Αιγαίου, (09.2007-02.2008).
- A.7.3.13 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Εμπορίου και Ανωόμενων Εταιρειών”, Siemens - Quality & Reliability – Οικονομικό Πανεπιστήμιο Αθηνών, 2006.
- A.7.3.14 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Ηλεκτρονικής Πολεοδομίας”, Singular Integrators – UniSystems – Οικονομικό Πανεπιστήμιο Αθηνών, 2006.
- A.7.3.15 **Αναλύτρια Επικινδυνότητας**, Έργο “Σχεδιασμός και υλοποίηση ελληνικής Αρχής Πιστοποίησης για την έκδοση ηλεκτρονικών διαβατηρίων”, D.S. Technologies - Οικονομικό Πανεπιστήμιο Αθηνών, 2006.
- A.7.3.16 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Ασφάλειας Ολοκληρωμένου Πληροφοριακού Συστήματος Υγείας ΔΥΠε Ιονίων Νήσων”, Κοινωνία της Πληροφορίας ΑΕ – Remaco ΑΕ – Οικονομικό Πανεπιστήμιο Αθηνών, 2006.
- A.7.3.17 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Ασφάλειας Πληροφοριακού Συστήματος Πυροσβεστικού Σώματος”, Quality and Reliability A.E. – Πανεπιστήμιο Αιγαίου, (1.2006 – 1.2007).
- A.7.3.18 **Ερευνήτρια**, Έργο, “Έλεγχος Συμβατότητας της Εταιρείας «ECDL Ελλάς» με το Πρότυπο ISO/IEC 27001”, CheckPoint, ECDL Hellas, 2006.

- A.7.3.19 **Αναλύτρια Επικινδυνότητας**, Έργο “Μελέτη Σχεδίου Ασφάλειας του Γενικού Νοσοκομείου Κορίνθου για τη λειτουργία αρχείων με ευαίσθητα δεδομένα”, ΓΝ Κορίνθου – Πανεπιστήμιο Αιγαίου, (11.2005 – 12.2005).
- A.7.3.20 **Ερευνήτρια**, Έργο e-UNIVERSITY: “Μελέτη, Καθορισμός Τεχνικών Προδιαγραφών-Τευχών Διαγωνισμών & Επίβλεψη Αναδόχου Υλοποίησης του Συστήματος Δημοσιεύσεων, Πληροφόρησης και Συναλλαγών του Πολίτη σε θέματα Διοικητικών Υποθέσεων και της Προμήθειας και Εγκατάστασης Δικτυακού και Υπολογιστικού Εξοπλισμού”, Κοινωνία της Πληροφορίας Α.Ε. – Πανεπιστήμιο Αιγαίου, (6.2005 – 12.2006).
- A.7.3.21 **Ερευνήτρια**, Έργο “Υλοποίηση του ελληνικού σήματος συμμόρφωσης/ποιότητας υπηρεσιών/δικτύων του ΕΛΟΤ”, ΕΛΟΤ – Οικονομικό Πανεπιστήμιο Αθηνών, 2005.

A.7.4 ΛΟΙΠΗ ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ

Ειδική Συνεργάτης του Ειδικού Γραμματέα Επιχειρησιακού Προγράμματος «Διοικητική Μεταρρύθμιση 2007-2013» του Υπουργείου Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης (12.2009-06.2011)

A.8 ΔΗΜΟΣΙΕΥΜΕΝΟ ΕΡΓΟ

A.8.1 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ ΜΕ ΣΥΣΤΗΜΑ ΚΡΙΤΩΝ

(Οι εκθέτες ανά άρθρο υποδηλώνουν τον αριθμό των ετεροαναφορών από μη συν-συγγραφείς)

- J. 16 Siponen, M. and Tsohou, A. (2017), Demystifying the influential IS legends of “positivism”, *Journal of the Association for Information Systems*, Accepted, ISI impact factor for 2016: 2.109
- J. 15 Tsohou, A. and Kosta, E. (2017), Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, Vol. 33, No. 4, pp. 434-457, ISI impact factor for 2016: 0.938
- J.14 ²² Tsohou A., Karyda M., Kokolakis S., (2015) Analyzing the role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs, *Computers & Security*, Vol. 52, pp. 128–141, ISI impact factor for 2015: 1.640
- J.13 Moon J.O., Lee H., Kim J.W., Aktas E., Tsohou A., Choi Y. (2015), Customer Satisfaction from Open Source Software Services in the Presence of Commercially Licensed Software, *Asia Pacific Journal of Information Systems*, Vol. 25, No. 3, pp. 473-499
- J.12 ¹⁹ Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2014) Managing the Introduction of

Information Security Awareness Programs in Organisations, *European Journal of Information Systems*, 24, pp. 38-58, [ISI impact factor for 2015: 2.892](#)

- J.11 ¹⁰ [Tsohou A.](#), Lee H., Irani A., (2014), Innovative Public Governance Through Cloud Computing: Information Privacy, Business Models And Performance Measurement Challenges, *Transforming Government: People, Process and Policy*, Vol. 8, No. 2, pp.251 – 282, Emerald.
- J.10 ¹ [Tsohou A.](#), Lee H., Irani Z., Weerakkody V., Osman I., and Anouze A., (2013), Proposing a Reference Process Model for the Citizen-Centric Evaluation of E-Government Services, *Transforming Government: People, Process and Policy*, Vol. 7, No. 2, pp. 240-255, Emerald
- J.09 ⁵ [Tsohou A.](#), Lee H., Al-Yafi K., Weerakkody V., El-Haddadeh R., Irani Z., Ko A., Medeni T., Campos L., (2012), Supporting Public Policy Making Processes with Workflow Technology: Lessons Learned From Cases in Four European Countries, *International Journal of Electronic Government Research*, Vol. 8, No. 3, pp.63-77, IGI Global
- J.08 ²¹ [Tsohou A.](#), Karyda M., Kokolakis S., Kiountouzis E., (2012), Analyzing Trajectories of Information Security Awareness, *Information Technology & People*, Vol. 25, Issue 3, 2012, Emerald, [ISI impact factor for 2015: 1.150](#)
- J.07 ²⁷ [Tsohou A.](#), Kokolakis S., Lambrinouidakis C., Gritzalis S., (2010), A security standards' framework to facilitate best practices' awareness and conformity, *Information Management & Computer Security*, Vol. 18, No. 5, pp. 350-365, Emerald
- J.06 ⁴ [Tsohou A.](#), Lambrinouidakis C., Kokolakis S., Gritzalis S., The Importance of Context Dependant Privacy Requirements and Perceptions to the Design of Privacy Aware Systems, *The European Journal of the Informatics Professional (UPGrade)*, Vol. XI, Issue 1, pp. 32-37.
- J.05 ⁵ [Tsohou A.](#), Karyda M., Kokolakis S., Kiountouzis E., (2010), Aligning Security Awareness with Information Systems Security Management, *Journal of Information System Security*, Vol. 6, No. 1, pp. 36-54.
- J.04 [Tsohou A.](#), Rizomiliotis P., Lambrinouidakis C., Gritzalis S., (2009), Security and Privacy Issues in Bipolar Disorder Research, *The Journal on Information Technology in Healthcare*, Vo. 7, No. 4, pp. 244-250
- J.03 ⁴⁷ [Tsohou A.](#), Kokolakis S., Karyda M., Kiountouzis E., (2008), Investigating information security awareness: research and practice gaps, *Information Security Journal: A Global Perspective*, Vol.17,

No. 5-6, pp. 207-227, Taylor and Francis

- J.02 ²⁴ Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., (2008), Process-Variance Models in Information Security Awareness Research, *Information Management and Computer Security*, Vol.16, No. 3, pp. 271 – 287, 2008, Emerald (Chosen as a Highly Commended Award Winner for Outstanding Paper at the Emerald Literati Network Awards for Excellence 2009).
- J.01 ⁵⁵ Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2006), Formulating Information Systems Risk Management Strategies through Cultural Theory, *Information Management and Computer Security*, Vol. 14, No. 3, pp. 198-217, Emerald

A.8.2 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ ΠΡΑΚΤΙΚΑ ΔΙΕΘΝΩΝ ΣΥΝΕΔΡΙΩΝ ΜΕ ΚΡΙΣΗ ΠΛΗΡΟΥΣ ΚΕΙΜΕΝΟΥ

(Οι εκθέτες ανά άρθρο υποδηλώνουν τον αριθμό των ετεροαναφορών από μη συν-συγγραφείς)

- C.17 Karavaras E., Magkos E. and Tsohou A. (2016) Low User Awareness Against Social Malware: an Empirical Study and Design of a Security Application, *In Proceedings of the 13th European, Mediterranean and Middle Eastern Conference on Information Systems*, June 2016, Krakow, Poland.
- C.16 Jiang H. and Tsohou A. (2015), The same Antecedents do not fit all activities: an Activity-Specific Model of Personal Internet Use in Workplace, (Research in Progress), *In Proceedings of the 23rd European Conference on Information Systems (ECIS 2015)*, May 2015, Mursten, Germany, Association for Information Systems (AIS)
- C.15 ⁶ Koufi V., Tsohou A., Malamateniou F. and Vassilacopoulos G., (2014), A Framework for Privacy-Preserving Access Control to Cloud Process-based PHR Systems, *25th European Medical Informatics Conference*, August 2014, Istanbul, Turkey.
- C.14 ¹ Jiang H. and Tsohou A. (2014), Expressive Or Instrumental: A Dual-Perspective Model Of Personal Web Usage At Workplace (Research in Progress) *In Proceedings of the 22nd European Conference on Information Systems (ECIS 2014)*, June 2014, Tel Aviv, Israel, Association for Information Systems (AIS)
- C.13 ³ Jiang H. and Tsohou A. (2014), The Dual Nature of Personal Web Usage At Workplace: Impacts, Antecedents And Regulating Policies, *In Proceedings of the 22nd European Conference on Information Systems (ECIS 2014)*, June 2014, Tel Aviv, Israel, Association for Information Systems (AIS)

- C.12 Oh J., Lee H. and Tsohou A. (2013) Relational Versus Structural Embeddedness in IT Outsourcing Networks: The Role Of Requirement Unpredictability And Measurement Difficulty, *17th Pacific Asia Conference on Information Systems (PACIS)*, June 2013, Jeju Island, Korea, Association for Information Systems (AIS)
- C.11 ¹ Tsohou A., Al-Yafi K., Lee H., (2012), Evaluating M-Government Applications: An Elaboration Likelihood Model Framework, *Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS)*, (Eds. Ghoneim A., Klischewski R., Schrödl H., Muhammed K.), 7-8 June, Munich, Germany
- C.10 Tsohou A., Lee H., Zahir I., Weerakkody V., Osman I., Latif A., Medeni T., (2012), Evaluating E-Government Services From A Citizens' Perspective: A Reference Process Model, *Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS)*, (Eds. Ghoneim A., Klischewski R., Schrödl H., Muhammed K.), 7-8 June, 2012, Munich, Germany
- C.09 ⁸ El-Haddadeh R., Tsohou A., Karyda M., (2012), Implementation Challenges for information Security Awareness initiatives in E-government, *Proceedings of the ECIS 2012 20th European Conference on Information Systems*, (Eds. Janssen M, Weerakkody V, Dwivedi Y), June 2012, Barcelona, Spain, Association for Information Systems (AIS)
- C.08 ² Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2010), Analyzing Information Security Awareness through Networks of Association, *Proceedings of the TrustBus 2010 7th International Conference on Trust, Privacy & Security in Digital Business*, pp. 227-237, September 2010, Bilbao, Spain, Lecture Notes in Computer Science LNCS, Springer
- C.07 ¹² Evans R., Tsohou A., Tryfonas T., Morgan T., (2010), Architecting Secure Systems with the ISO standards 26702 and 27001, *Proceedings of the SoSE 2010 5th IEEE International Conference on Systems of Systems Engineering*, pp. 1-6, June 2010, Loughborough, UK, IEEE Computer Society Press
- C.06 ⁶ Vrakas N., Kalloniatis C., Tsohou A., Lambrinouidakis C., (2010), Privacy Requirements Engineering for Trustworthy e-Government Services, *Proceedings of the TRUST 2010 3rd International Conference on Trust and Trustworthy Computing*, pp. 298-307, June 2010, Berlin, Germany, Lecture Notes in Computer Science LNCS, Springer
- C.05 ² Tsohou A., Kokolakis S., Lambrinouidakis C., Gritzalis S., (2010), Unifying ISO Security Standards Practices into a Single Security Framework, *Proceedings of the 12th Annual IFIP Workshop on*

Information Security Management, pp. 188-203, May 2010, Port Elizabeth, South Africa

- C.04 ¹⁴ Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2009), Aligning Security Awareness with Information Systems Security Management, *Proceedings of the MCIS 2009 4th Mediterranean Conference on Information Systems*, pp. 866- 878, September 2009, Athens, Greece, Association for Information Systems (AIS)
- C.03 ⁵ Tsohou A., Kokolakis S., Lambrinouidakis C., Gritzalis S., (2009), Information Systems Security Management: A review and a classification of the ISO standards, *Proceedings of the e-Democracy 2009 Next Generation Society: Technological and Legal Issues*, pp. 220-235, Athens, Greece, 2009, Lecture Notes of the ICSSIT Institute for Computer Sciences, Social Informatics, and Telecommunications Engineering LNICST 26, Springer
- C.02 Tsohou A., Rizomiliotis P., Lambrinouidakis C., Gritzalis S., (2009), Security and Privacy Issues in Bipolar Disorder Research, *Proceedings of the ICICTH 7th International Conference on Information and Communication Technologies in Health*, July 2009, Samos, Greece, INEAG
- C.01 ¹¹ Tsohou A., Theoharidou M., Kokolakis S., Gritzalis D., (2007), Addressing Cultural Dissimilarity in the Information Security Management Outsourcing Relationship, *Proceedings of the TRUSTBUS'07 4th International Conference on Trust, Privacy and Security in Digital Business*, pp.24-33, Regensburg, Germany, September 2007, Lecture Notes in Computer Science LNCS, Springer

A.8.3 ΔΗΜΟΣΙΕΥΣΕΙΣ ΣΕ WORKSHOPS, POSTERS ΚΑΙ ΠΕΡΙΑΗΨΕΙΣ ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ ΜΕ ΚΡΙΣΗ

- W.07 Grammenos, P., Syreggela, N.A., Magkos E. and Tsohou A. (2016), Internet Addiction of Young Greek Adults: Psychological Aspects and Information Privacy, In *Proceedings of the 2nd World Congress in Genetics, Geriatrics and Neurodegenerative Diseases Research*, Springer, Sparta, Greece, October 2016
- W.06 Papaioanou A. and Tsohou A. (2016), Social Networks as Education Tools: Aspects of Use and Privacy, In *Proceedings of the 8th Conference on Informatics in Education*, October 2016, Piraeus, Greece.
- W.05 Lee H. and Tsohou A. (2014), Can information systems intervene into citizens cognitive process to facilitate public participation? An elaboration likelihood model approach, *pre-ECIS SIGeGov workshop "Rethinking Information Systems in the Public Sector: Bridging Academia and Public*

Service", June 2014, Tel Aviv, Israel, Association for Information Systems (AIS).

- W.04 Tsohou A., Lee H., Weerakkody V., Irani Z., (2013), A Persuasive Information System for Policy Making: An Elaboration Likelihood Model Approach, *IT Management Worskhop*, 17th Pacific Asia Conference on Information Systems (PACIS), June 2013, Jeju Island, Korea, Association for Information Systems (AIS)
- W.03 Tsohou A. (2013), Innovative governance through cloud computing in public sector (OASIS-Openly Accessible Services and Interacting Society), *4th Transforming Government Workshop*, London, UK, March 2013
- W.02 Tsohou A., Lee H., and Barbos M., (2012), A location based persuasive information system for public consultation: An elaboration likelihood mode approach. *In the proceedings of 2nd international workshop on advanced service management*, Matsmoto, Japan, 29 – 30 Aug 2012
- W.01 Tsohou A., Lee H., Rebahi Y., Khalil M. and Hohberg S. (2012), Ubiquitous Participation Platform for POLicy Making (UbiPOL): Security and Identity Management Considerations, **Poster and Abstract In Proceedings of 9th Trust, Privacy and Security in Digital Business Conference (TrustBus 2012)**, (Eds. Fischer-Hübner S., Katsikas S. and Quirchmayr G.), Lecture Notes in Computer Science, Springer Berlin Heidelberg, Vol. 7449, p.p. 236-237, September, 2012, Vienna, Austria

A.8.4 ΔΙΑΤΡΙΒΕΣ

- T.02 Τσώχου Α., *Η Ενημερότητα Ασφάλειας στα Πλαίσια της Διοίκησης Ασφάλειας Πληροφοριακών Συστημάτων*, Διδακτορική Διατριβή, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου, Φεβρουάριος 2010
- T.01 Τσώχου Α., *Αντιλήψεις επικινδυνότητας στη Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων: Θεωρητικές προσεγγίσεις και παράγοντες διαμόρφωσης*, Μεταπτυχιακή Διατριβή, Μεταπτυχιακό σε Πληροφοριακά Συστήματα, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών, Φεβρουάριος 2004

A.9 ΠΡΟΣΚΕΚΛΗΜΕΝΕΣ ΟΜΙΛΙΕΣ

A.9.1 ΚΕΝΤΡΙΚΗ ΟΜΙΛΗΤΡΙΑ

- A.10.2.1 GDPR – A researcher’s view, **Executive Breakfast: GDPR - Security Solutions and Compliance**, 5th April 2017, PDMFC, IBM, Lisbon, Portugal

A.9.2 ΟΜΙΛΗΤΡΙΑ

- A.9.2.1 “Human behaviour change as a success factor for Internet information security”, **3rd Business Continuity Management Forum**, 15th December 2016, Netweek, Fidel & Fortis Ltd. Athens, Greece
- A.9.2.2 “Information privacy policies and Internet users’ privacy awareness” **ECSM Cyber Awareness Event**, 21st October 2016, ENISA, Piraeus, Greece

A.10 ΔΙΟΡΓΑΝΩΣΗ ΔΙΕΘΝΩΝ ΣΥΝΕΔΡΙΩΝ ΚΑΙ ΣΕΜΙΝΑΡΙΩΝ

A.10.1 ΔΙΟΡΓΑΝΩΣΗ ΘΕΡΙΝΩΝ ΣΧΟΛΕΙΩΝ

- A.10.1.1 **Διοργάνωση Θερινού Σχολείου**, Εντατικό Πρόγραμμα σε Ασφάλεια Πληροφοριών και Επικοινωνιακών Συστημάτων IPICS 2017, 28 Ιουνίου – 7 Ιουλίου 2017, Τμήμα Πληροφορικής, Κέρκυρα
- A.10.1.2 **Μέλος Οργανωτικής Επιτροπής**, Εντατικό Πρόγραμμα σε Ασφάλεια Πληροφοριών και Επικοινωνιακών Συστημάτων IPICS 2010, 17 Ιουλίου – 27 Ιουλίου 2010, Σάμος, Ελλάδα

A.10.2 ΔΙΟΡΓΑΝΩΣΗ ΣΥΝΕΔΡΙΩΝ ΚΑΙ WORKSHOPS

- A.10.2.1 **Μέλος Οργανωτικής Επιτροπής**, *STM 2010*, 6th International Workshop on Security and Trust Management, in conjunction with EuroPKI 2010 and CRITIS 2010, Athens, Greece, September 2010

A.11 ΣΥΝΤΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

A.11.1 ΜΕΛΟΣ ΣΥΝΤΑΚΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΠΕΡΙΟΔΙΚΩΝ

- A.11.1.1 *Internet Research, Emerald* (Editorial Board Member) (Έτος ένταξης 2011)
- A.11.1.2 *Information Management and Computer Security, Emerald* (Editorial Advisory Board Member) (Έτος ένταξης 2011)
- A.11.1.3 *Transforming Government: People, Process and Policy, Emerald* (Editorial Advisory Board Member) (Έτος ένταξης 2015)

A.11.2 ΜΕΛΟΣ ΣΥΝΤΑΚΤΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΠΕΡΙΟΔΙΚΩΝ – ΕΞΕΙΔΙΚΕΥΜΕΝΑ ΤΕΥΧΗ

- A.11.2.1 *Algorithms-SI 2016* Special Issue "Humanistic Data Processing" Algorithms Journal
- A.11.2.2 *CaEE-SI 2016* New Trends in Humanistic Informatics: Implementations and Applications, Computers & Electrical Engineering Journal
- A.11.2.3 *JoWUA 2013*, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications Journal

**A.11.3 ΜΕΛΟΣ ΕΠΙΣΤΗΜΟΝΙΚΗΣ ΕΠΙΤΡΟΠΗΣ
ΠΡΟΓΡΑΜΜΑΤΟΣ (PROGRAM COMMITTEE MEMBER) ΣΕ
ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ**

- A.11.3.1 *E-Democracy 2017*, 7th International Conference on e-Democracy, Athens, Greece, December 2017
- A.11.3.2 *COLLABORATECOM 2017* 3rd International Conference on Collaborative Computing: Networking, Applications and Worksharing, Guangzhou, China, November 2017
- A.11.3.3 *ESORICS 2017* 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 2017
- A.11.3.4 *PCI 2016*, 20th Panhellenic Conference on Informatics, Patra, Greece, November 2016
- A.11.3.5 *TrustBus 2016*, 13th International Conference on Trust, Privacy and Security in Digital Business, Porto, Portugal, September 2016
- A.11.3.6 *ESORICS 2016*, 21st European Symposium On Research In Computer Security, Crete, Greece, September 2016
- A.11.3.7 *SECRYPT 2016*, 13th International Conference on Security and Cryptography, Lisbon, Portugal, July 2016
- A.11.3.8 *E-Democracy 2015*, 7th International Conference on e-Democracy, Athens, Greece, December 2015
- A.11.3.9 *ARES 2015*, 10th International Conference on Trust, Privacy and Security in Digital Business, Toulouse, France, September 2015
- A.11.3.10 *TrustBus 2015* 12th International Conference on Trust, Privacy and Security in Digital Business, València, Spain, September 2015
- A.11.3.11 *PCI 2015*, 19th Panhellenic Conference on Informatics, Athens, Greece, October 2015
- A.11.3.12 *TrustBus 2014*, 11th International Conference on Trust, Privacy and Security in Digital Business, Munich, Germany, September, 2014
- A.11.3.13 *PCI 2014*, 18th Panhellenic Conference on Informatics, Athens, Greece, October 2014
- A.11.3.14 *ARES 2014*, 9th International Conference on Trust, Privacy and Security in Digital Business, Fribourg, Switzerland, September 2014
- A.11.3.15 *IADIS 2014*, 7th International Conference on Information Systems, Madrid, Spain, March 2014
- A.11.3.16 *ARES 2013*, 8th International Conference on Availability, Reliability and Security Regensburg, Germany, September 2013
- A.11.3.17 *TrustBus 2013*, 10th International Conference on Trust, Privacy and Security in Digital Business, Prague, Czech Republic, August 2013
- A.11.3.18 *IADIS 2013*, 7th International Conference on Information Systems, Lisbon, Portugal, March 2013
- A.11.3.19 *TrustBus 2012*, 9th International Conference on Trust, Privacy and Security in Digital Business, Vienna, Austria, September 2012

- A.11.3.20 *IEEE CloudCom 2011*, 3rd IEEE International Conference on Cloud Computing Technology and Science, Greece, Athens, December 2011
- A.11.3.21 *TrustBus 2011*, 8th International Conference on Trust, Privacy and Security in Digital Business, Toulouse, France, August, 2011
- A.11.3.22 *SECURITY 2010*, 7th International Conference on Security and Cryptography, Athens, Greece, July 2010
- A.11.3.23 *OTM IS 2010*, 5th International Symposium on Information Security, Crete, Greece, October 2010

A.11.4 ΚΡΙΤΗΣ (REVIEWER) ΕΡΕΥΝΗΤΙΚΩΝ ΕΡΓΑΣΙΩΝ ΣΕ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ

- A.11.4.1 *International Journal of Information Security*, Springer
- A.11.4.2 *Information & Management*, Elsevier
- A.11.4.3 *Communications of the Association for Information Systems*, Association for Information Systems
- A.11.4.4 *Behaviour & Information Technology*, Taylor & Francis
- A.11.4.5 *Information Technology & People*, Emerald
- A.11.4.6 *Computers and Security*, Elsevier.
- A.11.4.7 *Information Security Journal: A Global Perspective* (Previously published as: *Information Systems Security*), Taylor & Francis.
- A.11.4.8 *International Journal of Information Security*, Springer.
- A.11.4.9 *Transforming Government: People, Process and Policy*, Emerald.
- A.11.4.10 *Journal of Enterprise Information Management*, Emerald.
- A.11.4.11 *Asia Pacific Journal of Information Systems*, Korea Society of Management Information Systems
- A.11.4.12 *European Journal of Information Systems*, Palgrave
- A.11.4.13 *Journal of the Association of Information Systems*, Association for Information Systems
- A.11.4.14 *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, Innovative Information Science & Technology Research Group
- A.11.4.15 *International. Journal of Electronic Governance*, Inderscience Publishers

A.11.5 ΠΡΟΕΔΡΕΥΟΥΣΑ ΘΕΜΑΤΙΚΗΣ ΕΝΟΤΗΤΑΣ (TRACK CHAIR) ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ

- A.11.5.1 *MCIS 2017, 11th European Mediterranean & Middle Eastern Conference on Information Systems*, 5-6 September 2017, Genova, Italy, Track: **Trust, Security and Privacy**, Track Chairs: Maria Karyda and Aggeliki Tsohou
- A.11.5.2 *EMCIS 2017, 13th European Mediterranean & Middle Eastern Conference on Information Systems*, 7-8 September 2017, Coimbra, Portugal, Track: **Security and Privacy Protection for Information Systems and Digital services**, Track Chairs: Aggeliki Tsohou, Theo Tryfonas, Hemin Jiang

- A.11.5.3 *EMCIS 2016, 12th European Mediterranean & Middle Eastern Conference on Information Systems*, 1-2 June, Krakow, Poland, Track: **Security and Privacy Protection for Information Systems and Digital services**, Track Chairs: Aggeliki Tsohou, Ella Kolkowska
- A.11.5.4 *EMCIS 2015, 11th European Mediterranean & Middle Eastern Conference on Information Systems*, 1-2 June, Athens, Greece, Track: **Security and Privacy Protection for Information Systems and Digital services**, Track Chairs: Aggeliki Tsohou
- A.11.5.5 *EMCIS 2013, 10th European, Mediterranean & Middle Eastern Conference on Information Systems*, 17 – 18 October, Windsor, United Kingdom, **Track: Security and Privacy Protection for Information Systems**, Track Chairs: Aggeliki Tsohou, Costas Lambrinoudakis
- A.11.5.6 *AMCIS 2011, 18th Americas Conference on Information Systems*, Seattle, Washington August 9-11, 2012, **Mini-track: E-Government Trust and Information Security Issues and Concerns**, Mini-Track Chairs: Ramzi El-Haddadeh, Aggeliki Tsohou

A.11.6 ΚΡΙΤΗΣ (REVIEWER) ΕΡΕΥΝΗΤΙΚΩΝ ΕΡΓΑΣΙΩΝ ΣΕ ΔΙΕΘΝΗ ΣΥΝΕΔΡΙΑ

- A.11.6.1 *DPM 2016*, 11th International Workshop on Data Privacy Management, Heraklion, Crete, September 2016
- A.11.6.2 *ISSA 2016* 15th International Information Security South Africa Conference, Johannesburg, South Africa, August 2016
- A.11.6.3 *ECIS 2016*, 24th European Conference of Information Systems, Istanbul, Turkey, June 2016
- A.11.6.4 *IFIP SEC 2016*, 31th International Information Security and Privacy Conference, Ghent, Belgium, June 2016
- A.11.6.5 *SITIS 2015*, 11th International Conference on Signal Image Technology & Internet Based Systems, Bangkok, Thailand, November 2015
- A.11.6.6 *IFIPTM 2015*, 9th IFIP International Conference on Trust Management, Hamburg, Germany, May 2015
- A.11.6.7 *ISPEC 2015*, 11th International Conference on Information Security Practice and Experience, Beijing, China, May 2015
- A.11.6.8 *PCI 2015*, 19th Panhellenic Conference on Informatics, Athens, Greece, October 2015
- A.11.6.9 *E-Democracy 2015*, 6th International Conference on e-Democracy, Athens, Greece, December 2015
- A.11.6.10 *CRITIS 2015*, 10th International Workshop on Critical Information Infrastructures Security, Berlin, Germany, October 2015
- A.11.6.11 *ECIS 2015*, 23rd European Conference of Information Systems, Münster, Germany, May 2015
- A.11.6.12 *RCIS 2015*, 9th International Conference on Research Challenges in Information Science, Athens, Greece, May 2015
- A.11.6.13 *ECIS 2014*, 22nd European Conference on Information Systems, Tel Aviv, Israel, June 2014

- A.11.6.14 *CRITIS 2014*, 9th International Workshop on Critical Information Infrastructures Security, Limassol, Cyprus, October 2014
- A.11.6.15 *IFIPTM 2014*, 8th International Conference on Trust Management (IFIP WG 11.11), Singapore, July 2014
- A.11.6.16 *ICIS 2014*, 22nd International Conference on Information Systems, Auckland, New Zealand, December 2014
- A.11.6.17 *SEC 2014*, 29th International Information Security and Privacy Conference (IFIP TC-11 SEC), Marrakech, Morocco, June 2014
- A.11.6.18 *PACIS 2014* 18th Pacific Asia Conference on Information Systems, Chengdu, China, June 2014
- A.11.6.19 *PCI 2014*, 18th Panhellenic Conference on Informatics, Athens, Greece, October 2014
- A.11.6.20 *PACIS 2013*, 17th Pacific Asia Conference on Information Systems, Jeju Island, Korea, June 2013
- A.11.6.21 *ECIS 2013*, 21st European Conference on Information Systems, Utrecht, The Netherlands, June 2013
- A.11.6.22 *IEEE GLOBECOM ManSec-CC 2012*, 1st International workshop on Management and Security technologies for Cloud Computing, California, USA, December 2012
- A.11.6.23 *EMCIS 2012*, 9th European, Mediterranean and Middle Eastern Conference on Information Systems, Munich, Germany, June 2012
- A.11.6.24 *CAiSE 2011*, 23rd International Conference on Advanced Information Systems Engineering, London, UK, June 2011
- A.11.6.25 *WISTP 2011*, 5th Workshop in Information Security Theory and Practice, Heraclion, Greece, June 2011
- A.11.6.26 *IFIP SEC 2011*, 26th International Information Security Conference (IFIP TC-11), Luzern, Switzerland, June 2011
- A.11.6.27 *WMSCI 2010*, 14th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, Florida, USA, June 2010
- A.11.6.28 *CRITIS 2010*, 5th International Conference on Critical Information Infrastructure Security, Athens, Greece, September 2010
- A.11.6.29 *EGOVIS 2010*, 1st International Conference on Electronic Government and the Information Systems Perspective, Bilbao, Spain, September 2010.
- A.11.6.30 *ECIS 2010*, 18th European Conference on Information Systems, University of Pretoria, South Africa, June 2010
- A.11.6.31 *HAISA 2009*, 3rd International Symposium on Human Aspects of Information Security & Assurance, Athens, Greece, June 2009
- A.11.6.32 *ISSA 2009* Information Security Conference, Johannesburg, South Africa, July 2009

- A.11.6.33 *ESORICS 2008*, 13th European Symposium on Research in Computer Security, Malaga, Spain, October 2008
- A.11.6.34 *ISC 2008*, 11th Information Security Conference, Taipei, Taiwan, September 2008.
- A.11.6.35 *ICIS 2007*, 15th International Conference on Information Systems, Montréal, Québec, Canada, December 2007.
- A.11.6.36 *IADIS e-Commerce 2007*, 6th International Conference on e-Commerce, Algarve, Portugal, December 2007.

A.12 ΔΙΟΙΚΗΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

A.12.1 ΣΥΜΜΕΤΟΧΗ ΣΕ ΟΜΑΔΕΣ ΕΡΓΑΣΙΑΣ

Ιόνιο Πανεπιστήμιο, Τμήμα Πληροφορικής (2014 - Σήμερα)

- A. 12.1.1 Υπεύθυνη Σχεδιασμού του **Ωρολογίου Προγράμματος** Διαλέξεων και Εξεταστικής Προπτυχιακών Σπουδών (2014 - Σήμερα)
- A. 12.1.2 Υπεύθυνη Σχεδιασμού του **Ωρολογίου Προγράμματος** Διαλέξεων και Εξεταστικής Μεταπτυχιακών Σπουδών (2015 - Σήμερα)
- A. 12.1.3 Συμμετοχή στην Ομάδα Εργασίας **Ανασχεδιασμού της Χρήσης Κτιριακών χώρων και Υποδομών** του Τμήματος (2015)
- A. 12.1.4 Υπεύθυνη της Ομάδας Εργασίας για την **Επικαιροποίηση του Ιστοτόπου του Τμήματος** (2015 - Σήμερα)
- A. 12.1.5 Συμμετοχή στην Ομάδα Εργασίας **συντονισμού του Μεταπτυχιακού Προγράμματος Σπουδών Πληροφορική** (2015 – Σήμερα)
- A. 12.1.6 Συντονισμός της Ομάδα Εργασίας για τη **διοργάνωση Τελετής Αναγόρευσης** του Dr. Bernd Wegner σε επίτιμο διδάκτορα του Τμήματος Πληροφορικής του Ιονίου Πανεπιστημίου
- A. 12.1.7 Συμμετοχή στην Ομάδα Εργασίας για την προετοιμασία **Εξωτερικής Αξιολόγησης** του Ιονίου Πανεπιστημίου από την Αρχή Διασφάλισης και Πιστοποίησης της Ποιότητας στην Ανώτατη Εκπαίδευση (ΑΔΙΠ)

B. ΑΝΑΛΥΤΙΚΟ ΥΠΟΜΝΗΜΑ ΓΙΑ ΤΙΣ ΥΠΟΒΑΛΛΟΜΕΝΕΣ ΕΠΙΣΤΗΜΟΝΙΚΕΣ ΔΗΜΟΣΙΕΥΣΕΙΣ

B.1 ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Η ασφάλεια πληροφοριακών συστημάτων (Π.Σ.) προϋποθέτει την υλοποίηση τεχνικών αντιμέτρων, αλλά και την εφαρμογή οργανωτικών και διαδικαστικών μέτρων ασφάλειας. Όμως, όπως δείχνει η δημοσιευμένη έρευνα, ενώ η έρευνα των τεχνικών ζητημάτων έχει ήδη αποδώσει σε ένα μεγάλο πλήθος αποτελεσματικών εργαλείων και τεχνικών, ο άνθρωπος παραμένει ως ο “αδύναμος κρίκος” της αλυσίδας της ασφάλειας. Η συμμόρφωση με τους κανόνες, τις πολιτικές και τα μέτρα ασφάλειας δεν είναι εφικτή χωρίς τη διευθέτηση των ανθρωπίνων ζητημάτων της ασφάλειας. Μια από τις βασικές πρακτικές που προτείνονται για αυτό το σκοπό είναι οι πρωτοβουλίες ενημερότητας, κατάρτισης και εκπαίδευσης ασφάλειας Π.Σ. Οι σύγχρονες τεχνικές μελέτες για την ασφάλεια Π.Σ. αναγνωρίζουν την *ενημερότητα* ως ένα κρίσιμο παράγοντα στον οποίο πρέπει να εστιάσουν οι οργανώσεις για την αποτελεσματικότερη διοίκηση ασφάλειας Π.Σ.

Παρά το γεγονός ότι η σημασία της ενημερότητας ασφάλειας Π.Σ. αναγνωρίζεται από τους περισσότερους ερευνητές και οργανισμούς, η ενημερότητα παραμένει ένα από τα κρίσιμότερα ζητήματα των τελευταίων πέντε ετών σε σχέση με την ασφάλεια. Μάλιστα, η σπουδαιότητα της ενημερότητας ασφάλειας επισημαίνεται από το γεγονός ότι αναγνωρίζεται πως μπορεί να συνεισφέρει στην ενσωμάτωση της διοίκησης ασφάλειας Π.Σ. στη λειτουργία του οργανισμού. Παρά τον υψηλό βαθμό προτεραιότητας που της αποδίδεται οι οργανισμοί είναι διστακτικοί να αποδώσουν σημαντικές δαπάνες για σχετικές πρωτοβουλίες, ενώ συνηθίζεται να υλοποιούνται αποκομμένα από το ευρύτερο πλαίσιο διοίκησης ασφάλειας Π.Σ. Η διαπίστωση, λοιπόν, της αποσπασματικής ανάπτυξης και εφαρμογής πρωτοβουλιών ενημερότητας ασφάλειας και η αποκομμένη από τη διοίκηση ασφάλειας Π.Σ. αντιμετώπισή της από τους ερευνητές, αποτέλεσαν αφορμή για την έρευνα που παρουσιάζει η παρούσα διατριβή.

Το αντικείμενο της έρευνας που παρουσιάζει η διατριβή, είναι η *διαδικασία διαμόρφωσης και ενσωμάτωσης στρατηγικών ενημερότητας ασφάλειας σε μία οργάνωση*. Στόχος της διατριβής είναι η δημιουργία ενός εννοιολογικού και μεθοδολογικού πλαισίου που θα συνεισφέρει στην ανάλυση και κατανόηση των ενεργειών που λαμβάνουν χώρα κατά τη διαμόρφωση και υλοποίηση δραστηριοτήτων ενημερότητας ασφάλειας Π.Σ. και την εν συνεχεία ενσωμάτωσή τους στις λοιπές δραστηριότητες της διοίκησης ασφάλειας Π.Σ. Βασικά ερωτήματα στα οποία απαντά η έρευνα, είναι:

“Πώς γίνεται αποδεκτή και ενσωματώνεται μία δραστηριότητα ενημερότητας ασφάλειας πληροφοριακών συστημάτων σε ένα οργανωσιακό περιβάλλον;”

“Τι είδους αλλαγές επιδιώκει μια πρωτοβουλία ενημερότητας ασφάλειας;”

Η διατριβή ξεκινά με τη *μελέτη και κριτική ανάλυση της δημοσιευμένης έρευνας και πρακτικής* σχετικά με την ενημερότητα ασφάλειας πληροφοριακών συστημάτων που οδηγεί στην αναγνώριση α) των ανοικτών ζητημάτων στο χώρο της ενημερότητας ασφάλειας, και β) των προσεγγίσεων αναφορικά με τα μοντέλα έρευνας που εφαρμόζονται (θεωρίες μεταβλητότητας, θεωρίες διεργασιών,

υβριδικά μοντέλα). Η κριτική ανάλυση της βιβλιογραφίας, αναδεικνύει την απουσία κατάλληλου θεωρητικού υπόβαθρου και μεθοδολογικού πλαισίου των περισσότερων ερευνών ενημερότητας ασφάλειας Π.Σ.

Η *εμπειρική έρευνα* της διατριβής στηρίζεται σε μία σε βάθος μελέτη περίπτωσης, όπου διαμορφώνεται και υλοποιείται μία πρωτοβουλία ενημερότητας ασφάλειας σε πραγματικό οργανωσιακό περιβάλλον. Το *θεωρητικό πλαίσιο* για την ανάλυση και ερμηνεία των δεδομένων της έρευνας περιλαμβάνει τη θεωρία δικτύων σύμπραξης (actor network theory) για την ανάλυση σε μικρο-επίπεδο, τη θεωρία της δομοποίησης (structuration theory) για την ανάλυση σε μακρο-επίπεδο και τη θεωρία του συγκειμενισμού (contextualism) για τη σύνδεση της ανάλυσης σε μακρο-επίπεδο και μικρο-επίπεδο.

Η *θεωρία της δομοποίησης* εφαρμόζεται στο πεδίο των Π.Σ., με στόχο κυρίως τη μελέτη του ρόλου της τεχνολογίας στους οργανισμούς και τις δομές τους ή τη μελέτη φαινομένων στα οποία εμπλέκεται η τεχνολογία και επηρεάζει την ανθρώπινη δράση. Η εφαρμογή της θεωρίας της δομοποίησης επιτρέπει να μελετηθούν οι ενέργειες των εμπλεκόμενων μέσα στο πλαίσιο στο οποίο συμβαίνουν και να ερμηνευθεί η αλλαγή στα πλαίσια μίας οργάνωσης. Η *θεωρία του συγκειμενισμού* επιτρέπει την ανίχνευση της δυναμικής αλληλεπίδρασης των διαδικασιών αλλαγής και του εσωτερικού και εξωτερικού πλαισίου αναφοράς (συγκείμενο) με το περιεχόμενο της αλλαγής. Με αυτό τον τρόπο επιτρέπει την επεξήγηση του τρόπου με τον οποίο διαμορφώνεται το περιεχόμενο των αλλαγών από τις διαδικασίες αλλαγής λαμβάνοντας υπόψη τις συνθήκες του συγκεκριμένου περιβάλλοντος. Η *θεωρία δικτύων σύμπραξης* διερευνά τον τρόπο με τον οποίο οι άνθρωποι και τα τεχνουργήματα συνθέτουν ένα κοινωνικο-τεχνικό δίκτυο, μέσα από τη δράση ενός εστιακού δρώντος (focal actor). Επομένως, αναδεικνύει τον τρόπο με τον οποίο ανθρώπινα και μη ανθρώπινα στοιχεία συνεργάζονται και ενώνονται, διαμορφώνοντας ένα δίκτυο σύμπραξης. Η θεωρία δικτύων σύμπραξης, λοιπόν, παρέχει τη δυνατότητα ανάλυσης και ερμηνείας της διαδικασίας αλλαγής στο πλαίσιο μίας οργάνωσης ως μία διαδικασία διαπραγματεύσεων μεταξύ των συμμετεχόντων λαμβάνοντας υπόψη τις αντιλήψεις τους, τα συμφέροντά τους και το ρόλο που κατέχει στις διαπραγματεύσεις αυτές η τεχνολογία. Παράλληλα, η χρήση της *απαιτούμενης διαδικασίας* (due process) δίνει τη δυνατότητα παρακολούθησης της δυναμικής διαμόρφωσης του δικτύου αναδεικνύοντας τα κρίσιμα γεγονότα και οι οπτικές των συμμετεχόντων που καθορίζουν τη διαμόρφωση του δικτύου εστιάζοντας σε μεγαλύτερο βαθμό ανάλυσης.

Στα πλαίσια της διατριβής, λοιπόν, αναπτύσσεται *εννοιολογικό και μεθοδολογικό πλαίσιο* για την κατανόηση του τρόπου με τον οποίο διαμορφώνονται και ενσωματώνονται οι δράσεις ενημερότητας ασφάλειας Π.Σ. στις οργανώσεις. Η εφαρμογή του πλαισίου αυτού στην εμπειρική έρευνα οδήγησε σε τεκμηριωμένα συμπεράσματα που απευθύνονται τόσο στους ερευνητές, όσο και ειδικούς του χώρου της ασφάλειας των Π.Σ. Η *συμβολή* της έρευνας έχει θεωρητική, μεθοδολογική και πρακτική διάσταση:

- ✓ Σε *θεωρητικό επίπεδο*, τα συμπεράσματα της έρευνας επισημαίνουν την καταλληλότητα της θεωρίας δικτύων σύμπραξης για τη δυναμική παρακολούθηση της διαμόρφωσης της ενημερότητας ασφάλειας Π.Σ. και τον κρίσιμο ρόλο των ικανοτήτων και δεξιοτήτων του εστιακού δρώντα να ‘ευθυγραμμίσει’ τα συμφέροντα των δυνητικών συμμάχων με τα

συμφέροντα του δικτύου. Ο συνδυασμός της θεωρίας δικτύων σύμπραξης με τη θεωρία δομοποίησης συνεισφέρει στην κατανόηση του τρόπου με τον οποίο ένας δρων που δραστηριοποιείται στο μικρο-επίπεδο μπορεί να συνεισφέρει στη δημιουργία ενός νέου δικτύου σύμπραξης σε υψηλότερο επίπεδο, ενώ η θεωρία του συγκειμενισμού μπορεί να συντελέσει στην κατανόηση των συνθηκών του ευρύτερου πλαισίου που επιδρούν στη διαμόρφωση των δικτύων σύμπραξης σε μικρο-επίπεδο και μακρο-επίπεδο.

- ✓ Σε *πρακτικό επίπεδο*, το εννοιολογικό και μεθοδολογικό πλαίσιο της διατριβής μπορεί να αξιοποιηθεί ως πλαίσιο αναφοράς από ειδικούς ασφάλειας Π.Σ. που σχεδιάζουν να αναπτύξουν πρωτοβουλίες ενημερότητας, ώστε να εντοπίσουν ‘κρίσιμα’ γεγονότα κατά τη διαρκή διαμόρφωση του δικτύου σύμπραξης καθώς και τα σημεία όπου το δίκτυο μπορεί να αποσταθεροποιηθεί και για ποιες αιτίες. Ακόμη, πληροφορεί τους ειδικούς ασφάλειας Π.Σ. αναφορικά με τις πρόσθετες δεξιότητες που αναδεικνύεται ότι απαιτούνται για την αποτελεσματική διαχείριση μίας τέτοιας δραστηριότητας, όπως επικοινωνιακές, διαπραγματευτικές και διοικητικές δεξιότητες. Τέλος, επισημαίνεται η μη ουδετερότητα των τεχνουργημάτων αναφορικά με την επιρροή τους σε τέτοιες πρωτοβουλίες.
- ✓ Σε *μεθοδολογικό επίπεδο*, αρχικά οι ερευνητές χώρου της ασφάλειας, αλλά και των Π.Σ. γενικότερα, μπορούν να επωφεληθούν από την εφαρμογή της τυπολογίας μοντέλων έρευνας, κατά το σχεδιασμό της έρευνάς τους. Ακόμη, τα συμπεράσματα της έρευνας αναδεικνύουν τη συμβατότητα και συμπληρωματικότητα των τριών θεωριών για την κατανόηση και ανάλυση της ενημερότητας ασφάλειας Π.Σ.

B.2 ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ ΔΗΜΟΣΙΕΥΜΕΝΕΣ ΣΕ ΔΙΕΘΝΗ ΕΠΙΣΤΗΜΟΝΙΚΑ ΠΕΡΙΟΔΙΚΑ

- J. 16 *Siponen, M. and Tsohou, A. (2017), Demystifying the influential IS legends of “positivism”, Journal of the Association for Information Systems, Accepted, ISI impact factor for 2016: 2.109*

Positivism has been used to establish a standard that IS research must meet to be scientific. According to such positivistic beliefs in IS, scientific research should: 1) be generalizable; 2) focus on stable independent variables; 3) have certain ontological assumptions; and 4) use surveys rather than qualitative methods. We argue that logical positivist philosophers required none of these. On the contrary, logical positivist philosophers regarded philosophizing in general and ontological considerations in particular as nonsense. Moreover, the positivists’ preferred empirical research method was not a survey, but rather a qualitative observation recorded by field notes. In addition, positivist philosophers neither required statistical nor non-statistical generalizability. Many positivist philosophers also acknowledged the study of singular cases as being scientific.

Many research orientations (e.g., single-setting research, examination of change, qualitative

research) that are deemed as unscientific in IS seem to be (in principle) “scientific” according to logical positivism. In turn, what has been justified as scientific by positivism in IS (e.g., requirements of statistical or non-statistical generalizability, surveys, focus on fixed things, ontological views) either were not required by logical positivists or were regarded as nonsensical by logical positivists. Furthermore, given that positivism is sometimes associated (or confused) with logical empiricism in IS, we also briefly discuss logical empiricism. Finally, realizing that certain influential, taken-for-granted assumptions that underlie IS research are unwarranted, could have ground-breaking implications for future IS research.

- J.15 *Tsohou, A. and Kosta, E. (2017), Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 33, No. 4, pp. 434-457, ISI impact factor for 2016: 0.938*

People use mobile devices for an increasing variety of purposes in order to enjoy the vast possibilities; they check the local weather, road traffic, personalised local news, their personalised favourite social network etc. At the same time, application developers and market stores deploy mobile applications that collect vast amounts of information on mobile users, such as their age, gender, location or specific phone identifiers. Numerous studies illustrate that mobile applications collect valuable information about users and use it for profiling the users for their own purposes or sell this information for commercial interests. Therefore, the topic of consent to information processing becomes increasingly more interesting for researchers, legal experts and practitioners.

In this paper, the authors examine the issue of valid informed consent for location tracking by mobile phone users. They first analyse the legal premises for informed consent that represent requirements for mobile application developers and providers who request consent. However, the ones who actually give consent are the mobile users and therefore their understanding of consent is of paramount importance. Extensive literature is missing on empirical studies examining the topic from the users’ perception perspective. For that reason, the authors conduct an empirical investigation with mobile users and present their findings in the form of a process theory. The process theory reveals how users’ valid informed consent for location tracking can be obtained, starting from enhancing reading the privacy policy to stimulating privacy awareness and enabling informed consent. The paper includes a

discussion section in which the authors describe the implications of the process theory for the different stakeholders and offer recommendations deriving from the empirical findings. The contribution is addressed to software and mobile application developers and providers, technology regulation researchers and policy makers, as well as security and privacy researchers.

- J. 14 *Tsohou A., Karyda M., Kokolakis S., (2015) Analyzing the role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs, Computers & Security, Vol. 52, pp. 128–141*

Τίτλος: «Αναλύοντας το ρόλο των Γνωστικών και Πολιτισμικών Προδιαθέσεων στην Εσωτερικευση των Πολιτικών Ασφάλειας Πληροφοριών: Συστάσεις προς την Ανάπτυξη Προγραμμάτων Ενημερότητας Ασφάλειας»

Τα πρότυπα και οι βέλτιστες πρακτικές που υπάρχουν για την καθοδήγηση στο σχεδιασμό και την υλοποίηση προγραμμάτων ενημερότητας ασφάλειας πληροφοριών εστιάζουν στο ποιο θα πρέπει να είναι το περιεχόμενο αυτών των προγραμμάτων, χωρίς να λαμβάνουν υπόψη τον τρόπο με τον οποίο τα άτομα λαμβάνουν και επεξεργάζονται αυτό το περιεχόμενο και πώς το αξιοποιούν για την καθημερινή λήψη των αποφάσεών τους στον εργασιακό χώρο. Η πρόσφατη βιβλιογραφία παρόλα αυτά έχει αποδείξει ότι η τελική συμμόρφωση των χρηστών στις πολιτικές ασφάλειας επηρεάζεται από τις αντιλήψεις του ατόμου για την επικινδυνότητα, τις πεποιθήσεις του και τις προδιαθέσεις του. Επομένως τα προγράμματα ενημερότητας θα πρέπει να ευθυγραμμιστούν με αυτούς τους παράγοντες που καθορίζουν τον τρόπο με τον οποίο οι χρήστες ενστερνίζονται τα μηνύματα ασφάλειας πληροφοριών που μεταδίδονται. Η εργασία αυτή μελετά το ρόλο των γνωστικών (cognitive) και πολιτισμικών (cultural) προδιαθέσεων στη διαμόρφωση των αντιλήψεων επικινδυνότητας και των συμπεριφορών σε σχέση με την ασφάλεια. Η εργασία αξιοποιεί βιβλιογραφία από διαφορετικά πεδία, όπως οικονομικά της συμπεριφοράς (behavioural economics) και προσωπική ασφάλεια (safety) προκειμένου να αναπτύξει ένα εννοιολογικό πλαίσιο για την ανάλυση του ρόλου των γνωστικών και πολιτισμικών προδιαθέσεων του ατόμου στην ασφάλεια πληροφοριών. Στο πλαίσιο της εργασίας αναλύονται οι επιπτώσεις αυτών των προδιαθέσεων για τα προγράμματα ενημερότητας και τελικά παρέχουμε ένα σύνολο από συστάσεις προς τους αρμόδιους σχεδιασμού και υλοποίησης προγραμμάτων ενημερότητας της ασφάλειας. Η εργασία αναδεικνύει νέες οδούς για την έρευνα στο πεδίο της

ενημερότητας ασφάλειας και των αποφάσεων ασφάλειας πληροφοριών, ενώ προτείνει πρακτικές συστάσεις για την υλοποίηση προγραμμάτων ενημερότητας αξιοποιώντας το ρόλο των προδιαθέσεων στη διαμόρφωση των αντιλήψεων επικινδυνότητας και των συμπεριφορών των χρηστών σε σχέση με την ασφάλεια.

- J.13 *Moon J.O., Lee H., Kim J.W., Aktas E., Tsohou A., Choi Y. (2015), Customer Satisfaction from Open Source Software Services in the Presence of Commercially Licensed Software, Asia Pacific Journal of Information Systems, Vol. 25, No. 3, pp. 473-499*

Τίτλος: «Ικανοποίηση των Πελατών από Λογισμικό Ανοικτού Κώδικα με την Παρουσία Εμπορικού Λογισμικού»

Η βιβλιογραφία που αφορά στην υιοθέτηση λογισμικού ανοικτού κώδικα είναι περιορισμένη και δεν παρέχει επεξηγήσεις για τον τρόπο με τον οποίο υιοθετούνται από τους καταναλωτές, στην περίπτωση που υπάρχει διαθέσιμο εμπορικό λογισμικό που υπερέχει λειτουργικά. Η εργασία αποσκοπεί στην αποκάλυψη της διαδικασίας με την οποία διαμορφώνεται η ικανοποίηση του καταναλωτή από λογισμικό ανοικτού κώδικα σε σχέση με το εμπορικό λογισμικό. Υιοθετούμε τη θεωρία διάψευσης προσδοκιών (Expectation Disconfirmation Theory) ενσωματώνοντας παράγοντες κόστους, φήμης και προσωπικής εμπειρίας. Το μοντέλο που σχεδιάστηκε στην εργασία επικυρώνεται με εμπειρικά δεδομένα από έρευνα πεδίου στην Κορέα μεταξύ ενός συστήματος διαχείρισης βάσεων δεδομένων ανοικτού κώδικα και αντίστοιχου συστήματος στην αγορά που υπερέχει λειτουργικά. Η θεωρητική συνεισφορά της εργασίας συνίσταται στην εφαρμογή της θεωρίας διάψευσης προσδοκιών για τη σύγκριση της υιοθέτησης των δύο συστημάτων. Επιπλέον, η εργασία ενσωματώνει παράγοντες σχετικούς με τις προσδοκίες των καταναλωτών, το οποίο είχε αναγνωριστεί στη βιβλιογραφία ως ερευνητικό κενό. Η πρακτική συνεισφορά της εργασίας συμπεριλαμβάνει την αναγνώριση των διαφορών ανάμεσα στις προσδοκίες των χρηστών από λογισμικό ανοικτού κώδικα και εμπορικό λογισμικό. Τέλος η εργασία παρέχει επεξηγήσεις για τον τρόπο με τον οποίο οι αρχικές προσδοκίες των καταναλωτών συνδυάζονται με την προσωπική τους εμπειρία από τη χρήση του λογισμικού προς τη διαμόρφωση του βαθμού ικανοποίησής τους.

- J.12 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2014) Managing the Introduction of Information Security Awareness Programs in Organisations, European Journal of Information Systems, 24, pp. 38-58*

Τίτλος: «Η Διαχείριση της Εισαγωγής Προγραμμάτων Ενημερότητας Ασφάλειας Πληροφοριών στους Οργανισμούς»

Η βιβλιογραφία περιλαμβάνει διάφορες εργασίες που διερευνούν το ζήτημα της ενημερότητας ασφάλειας πληροφοριών εστιάζοντας στο ατομικό ή/και το οργανωσιακό επίπεδο. Σε αυτή την εργασία ισχυριζόμαστε ότι οι διαδικασίες της ενημερότητας ασφάλειας πληροφοριών συσχετίζονται με αλληλεξαρτώμενες αλλαγές που συμβαίνουν τόσο στο ατομικό και το οργανωσιακό αλλά και το τεχνολογικό επίπεδο. Προτείνουμε ένα ολοκληρωμένο θεωρητικό πλαίσιο ανάλυσης το οποίο αναπτύχθηκε με χρήση έρευνας παρεμβάσεων (action research) σε ένα δημόσιο οργανισμό. Το πλαίσιο ενσωματώνει τη θεωρία δικτύων σύμπραξης, τη θεωρία δομοποίησης και τη θεωρία του συγκειμενισμού. Στην εργασία αναπτύσσουμε και εφαρμόζουμε το πλαίσιο για την υλοποίηση ενός προγράμματος ενημερότητας ασφάλειας πληροφοριών και τη διαχείριση των αλλαγών που προκύπτουν στον φορέα οργανισμό. Η εργασία αναδεικνύει τις ελλείψεις που έχει η κάθε μία θεωρία εάν εφαρμοστεί μόνη της για την ανάλυση αλλαγών σε πολλαπλά επίπεδα (multi-level changes), ενώ καταδεικνύει τη συνέργεια που προκύπτει από το συνδυασμό τους. Η εργασία προτείνει πώς το πλαίσιο μπορεί να εφαρμοστεί για την μελέτη και ανάλυση αλλαγών που σχετίζονται με την ενημερότητα ασφάλειας πληροφοριών και προκύπτουν σε ατομικό, οργανωσιακό και τεχνολογικό επίπεδο.

- J.11 *Tsohou A., Lee H., Irani A., Innovative Public Governance Through Cloud Computing: Information Privacy, Business Models And Performance Measurement Challenges, Transforming Government: People, Process and Policy, Vol. 8, No. 2, Emerald.*

Τίτλος: «Καινοτομία στην Δημόσια Διοίκηση μέσω Τεχνολογιών Νεφοϋπολογιστικής: Προκλήσεις για την Προστασία της Ιδιωτικότητας, τα Επιχειρησιακά Μοντέλα και την Μέτρηση Αποτελεσματικότητας»

Σκοπός: Οι καινοτόμες τεχνολογίες, όπως η νεφοϋπολογιστική, φέρουν τη δυνατότητα να συνεισφέρουν στην παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης, μέσα από ευέλικτα και επεκτάσιμα συστήματα. Επιπλέον, μπορούν να ενισχύσουν την μείωση κόστους και να μειώσουν την κατάρτιση των δημόσιων πληροφοριών. Παρόλα αυτά, όταν οι δημόσιες υπηρεσίες αξιοποιούν αυτές τις τεχνολογίες αντιμετωπίζουν σημαντικά προβλήματα που σχετίζονται με τις συνοδευόμενες τεχνικές και οργανωσιακές αλλαγές, καθώς και άλλες προκλήσεις. Ο σκοπός αυτής της εργασίας είναι να αναγνωρίσει και να αναλύσει αυτές τις

προκλήσεις και να συζητήσει προτεινόμενες λύσεις.

Μεθοδολογία και Σχεδιασμός Έρευνας: Ακολουθήσαμε μία διεπιστημονική προσέγγιση, συμπεριλαμβάνοντας κοινωνικά, συμπεριφορικά, επιχειρησιακά και τεχνικά στοιχεία, και βιβλιογραφική ανάλυση των προκλήσεων. Πραγματοποιήσαμε συνεντεύξεις ομάδων εργασιών (focus group interviews) σε δύο χώρες για την αξιολόγηση της επίδοσης των μοντέλων που προέκυψαν ως αποτέλεσμα της βιβλιογραφικής ανάλυσης.

Ευρήματα: Η εργασία αναγνωρίζει και αναλύσει διάφορες τις προκλήσεις που μπορεί να αναδυθούν κατά την υιοθέτηση καινοτόμων τεχνολογιών στη δημόσια διακυβέρνηση και τις υπηρεσίες ηλεκτρονικής διακυβέρνησης. Επιπλέον παρουσιάζει προτεινόμενες λύσεις οι οποίες έχουν εξαχθεί από την εμπειρία σχεδιασμού και υλοποίησης μία σχετικής πλατφόρμας δημόσιας διακυβέρνησης με χρήση τεχνολογιών νεφοϋπολογιστικής, συμπεριλαμβανομένων απαιτήσεων προστασίας της ιδιωτικότητας, επιχειρησιακά μοντέλα, μετρικές αποτίμησης απόδοσης για τις δημόσιες υπηρεσίες.

Περιορισμοί της έρευνας: Οι προκλήσεις και οι λύσεις που αναλύονται στο πλαίσιο της εργασίας βασίζονται στην εμπειρία σχεδιασμού και υλοποίησης μίας πλατφόρμας. Παρόλα αυτά, θα πρέπει να σημειωθεί ότι η πλατφόρμα αυτή συμπεριέλαβε δημόσιες υπηρεσίες από 4 χώρες.

Καινοτομία/Συνεισφορά: Αυτή η εργασία αποτελεί την πρώτη μελέτη που συζητά τις προκλήσεις αξιοποίησης τεχνολογιών νεφοϋπολογιστικής για τη δημόσια διακυβέρνηση λαμβάνοντας υπόψη πολλαπλές οπτικές και μέσω εμπειρικής έρευνας. Η εμπειρική έρευνα αφορά σε υπηρεσίες που θα αξιοποιηθούν σε μία πλατφόρμα που θα λειτουργήσει σε Ευρωπαϊκό επίπεδο.

- J.10 *Tsohou A., Lee H., Irani Z., Weerakkody V., Osman I., and Anuze A. (2013), Proposing a Reference Process Model for the Citizen-Centric Evaluation of E-Government Services, Transforming Government: People, Process and Policy, Vol. 7, No. 2, pp. 240-255, Emerald*

Τίτλος: « Προτείνοντας ένα Διεργασιακό Μοντέλο Αναφοράς για την Πολιτο-Κεντρική Αξιολόγηση των Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης»

Η αξιολόγηση και βελτιστοποίηση των υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι απαραίτητη για τις κυβερνήσεις ειδικά δεδομένων των δυνατοτήτων των ηλεκτρονικών υπηρεσιών να μεταρρυθμίσουν τη δημόσια διοίκηση και να βοηθήσουν στην αλληλεπίδραση της Πολιτείας και των πολιτών, των επιχειρήσεων και των δημόσιων φορέων. Από τις

υπάρχουσες προσεγγίσεις αξιολόγησης απουσιάζουν μετρικές μέτρησης της ικανοποίησης των πολιτών. Ο σκοπός αυτής της εργασίας είναι διττός: να συνεισφέρει στην κατανόηση της πολιτοκεντρικής αξιολόγησης των υπηρεσιών ηλεκτρονικής διακυβέρνησης ενσωματώνοντας υπάρχουσες μετρικές κλειδιά για την απόδοση, και να προτείνει ένα πρότυπο διεργασιακό μοντέλο για μία καινοτόμα προσέγγιση αξιολόγησης που εφαρμόζει τις μετρικές αυτές προκειμένου να διευκολύνει τη δημιουργία βάσης γνώσης. Υιοθετήσαμε μία ποσοτική ερευνητική προσέγγιση για την αξιολόγηση των υπηρεσιών ηλεκτρονικής διακυβέρνησης βασισμένη στην τεχνική ανάλυσης φακέλου δεδομένων (Data Envelope Analysis). Για την εμπειρική έρευνα πραγματοποιήθηκε δημοσκόπηση και συλλέχθηκαν δεδομένα για 13 υπηρεσίες ηλεκτρονικής διακυβέρνησης στην Τουρκία. Με βάση την εμπειρική έρευνα σχεδιάστηκε το προτεινόμενο πρότυπο διεργασιακό μοντέλο. Η προτεινόμενη προσέγγιση αξιολόγησης αποδείχθηκε έγκυρη και ικανή να παρέχει αποτίμηση και επεξηγήσεις πλουσιότερες από τις παραδοσιακές στατιστικές μετρικές. Η τεχνική ανάλυσης φακέλου δεδομένων ενεργοποίησε την αναγνώριση μη αποδοτικών υπηρεσιών ηλεκτρονικής διακυβέρνησης και την παροχή σχετικών προτάσεων διόρθωσης. Το πρότυπο διεργασιακό μοντέλο κατασκευάστηκε λαμβάνοντας υπόψη την εμπειρία από την εφαρμογή της μεθόδου σε ένα μόνο πολιτισμικό περιβάλλον (της Τουρκίας). Η προτεινόμενη μέθοδος αξιολόγησης παρείχε πιο πλούσιες αποτιμήσεις σε σχέση με άλλες ανθρωποκεντρικές και στατιστικές μεθόδους. Το προτεινόμενο πρότυπο μοντέλο αναμένεται να επιταχύνει την εφαρμογή πολιτοκεντρικής αξιολόγησης υπηρεσιών ηλεκτρονικής διακυβέρνησης και να ενισχύσει την εφαρμογή μετρικών επιπτώσεων. Η εργασία αυτή αποτελεί την πρώτη εφαρμογή της τεχνικής ανάλυσης φακέλου δεδομένων στο πεδίο της ηλεκτρονικής διακυβέρνησης. Η καινοτομία της τεχνικής είναι ότι τα αποτελέσματα της αξιολόγησης παρέχουν προτάσεις για στρατηγικές βελτιώσεις των υπηρεσιών.

- J.9 *Tsohou A., Lee H., Al-Yafi K., Weerakkody V., El-Haddadeh R., Irani Z., Ko A., Medeni T., Campos L., “Supporting Public Policy Making Processes with Workflow Technology: Lessons Learned From Cases in Four European Countries”, International Journal of Electronic Government Research, Vol. 8, No. 3, 2012, IGI Global.*

Τίτλος: «Υποστηρίζοντας τις Διαδικασίες Διαμόρφωσης Δημόσιων Στρατηγικών μέσω Τεχνολογιών Ροής Εργασίας: Διδάγματα από Μελέτες Περίπτωσης σε τέσσερις Ευρωπαϊκές Χώρες»

Τα συστήματα ροής εργασιών έχουν καταστήσει εφικτά πολλαπλά οφέλη για ιδιωτικούς και δημόσιους οργανισμούς, συμπεριλαμβανομένων μείωσης κόστους, αύξηση αποδοτικότητας, αύξηση ικανοτήτων, αύξηση ταχύτητας επεξεργασίας, μείωση λαθών, αύξηση ποιότητας υπηρεσιών και αύξηση ικανοποίησης πελατών. Ο δημόσιος τομέας έχει εκμεταλλευτεί αυτά τα πλεονεκτήματα εφαρμόζοντας συστήματα διοίκησης ροής εργασιών για την υποστήριξη των διοικητικών διαδικασιών, όπως διαχείριση ανθρώπινων πόρων. Παρόλα αυτά, η τεχνολογία αυτή δεν έχει ακόμη αξιοποιηθεί για την υποστήριξη των διαδικασιών σχεδιασμού πολιτικής, κάτι που θα αναμενόταν ότι να ενισχύσει τη συμμετοχή των πολιτών στις διαδικασίες σχεδιασμού δημόσιων πολιτικών και να ενισχύσει την ενημερότητά τους σε δημόσια ζητήματα. Ο στόχος αυτής της εργασίας είναι να διερευνήσει τη δυνατότητα υιοθέτησης εργαλείων αυτοματοποίησης ροών εργασίας για την υποστήριξη των διαδικασιών λήψης αποφάσεων στο πλαίσιο δημόσιων πολιτικών, ανεξάρτητα από το θεσμικό πλαίσιο. Για αυτό το σκοπό αναλύονται οι διαδικασίες σχεδιασμού δημόσιων πολιτικών σε τέσσερις χώρες. Τα ευρήματα υποδεικνύουν ότι οι διαδικασίες σχεδιασμού έχουν σημαντικά κοινά στοιχεία, ακόμη κι αν ανήκουν σε διαφορετικά πεδία πολιτικής και διαφορετικά θεσμικά πλαίσια, γεγονός που αφήνει ανοικτή τη δυνατότητα αξιοποίησης των τεχνολογιών αυτοματοποίησης ροών εργασίας στην υποστήριξη των διαδικασιών σχεδιασμού δημόσιων πολιτικών.

- J.8 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., (2012) Analyzing Trajectories of Information Security Awareness, Information Technology & People, Vol. 25, Issue 3, Emerald*

Τίτλος: «Αναλύοντας τους Μετασχηματισμούς την Ενημερότητας Ασφάλειας»

Οι πρόσφατες διεθνείς έρευνες καταδεικνύουν ότι τα προγράμματα ενημερότητας και κατάρτισης δεν είναι όσο αποτελεσματικά θα μπορούσαν να είναι και ότι οι επενδύσεις των οργανισμών σε σχετικά προγράμματα δεν είναι κατάλληλες. Ο σκοπός της παρούσας εργασίας είναι να ενισχύσει την κατανόησή μας για αυτό το φαινόμενο και να αναδείξει τα προβλήματα που αντιμετωπίζουν οι οργανισμοί όταν επιχειρούν την υλοποίηση ενός προγράμματος ενημερότητας ασφάλειας πληροφοριών. Υιοθετούμε την ερμηνευτική προσέγγιση και υλοποιούμε μία περίπτωση μελέτης (case study) εφαρμόζοντας τη θεωρία των δικτύων σύμπραξης (Actor Network Theory) και την τεχνική της απαιτούμενης διαδικασίας (due process) προκειμένου να αναλύσουμε τα δεδομένα μας. Η εργασία αυτή

συνεισφέρει τόσο μέσω της κατανόησης και διαχείρισης προγραμμάτων ενημερότητας ασφάλειας σε οργανισμούς όσο και μέσω της παροχής ενός πλαισίου για την ανάλυση της αλληλεπίδρασης μεταξύ των ενεργειών ενός προγράμματος ενημερότητας με τις διάφορες διαδικασίες και γεγονότα του οργανισμού φορέα.

Η εφαρμογή της θεωρίας δικτύων σύμπραξης είναι πρόκληση για τους ερευνητές καθώς δεν υπάρχει καμία μέθοδος πρακτικής εφαρμογής ή καθοδήγηση για την εφαρμογή της. Σε αυτή την εργασία διευκολύνουμε την εφαρμογή της θεωρίας και παρέχουμε πρακτική καθοδήγηση πώς μπορεί να εφαρμοστεί μέσω της επέκτασης με την τεχνική της απαιτούμενης διαδικασίας. Η έρευνά μας αναδεικνύει το γεγονός ότι τα προγράμματα ενημερότητας ασφάλειας συμπεριλαμβάνουν πολλούς εμπλεκόμενους, οι οποίοι πολλές φορές έχουν αντικρουόμενα συμφέροντα. Οι επαγγελματίες ασφάλειας θα πρέπει να κατέχουν, πρόσθετα των τεχνικών γνώσεων και ικανοτήτων, και δεξιότητες επικοινωνίας, διαπραγμάτευσης και διοίκησης, προκειμένου να διευθετήσουν όλα τα σχετικά οργανωσιακά και διοικητικά ζητήματα. Επιπρόσθετα, τα αποτελέσματα της έρευνάς μας αποκαλύπτουν ότι ο ρόλος των τεχνουργημάτων σε ένα πρόγραμμα ενημερότητας ασφάλειας δεν είναι ουδέτερος αλλά αντίθετα μπορούν να επηρεάσουν ενεργά το πρόγραμμα. Αυτή η έρευνα είναι μία από τις πρώτες που εξετάζουν τα προγράμματα ενημερότητας ασφάλειας ως μια διοικητική και κοινωνικο-τεχνική διαδικασία σε ένα οργανωσιακό πλαίσιο.

- J.7 *Tsohou A., Kokolakis S., Lambrinouidakis C., Gritzalis S., “A Framework of Security Standards to Facilitate Best Practices’ Awareness and Conformity”, Information Management & Computer Security, Vol. 18, No. 5, 2010.*

Τίτλος: «Ένα Πλαίσιο Προτύπων Ασφάλειας για την Υποστήριξη της Ενημερότητας και Συμμόρφωσης με Βέλτιστες Πρακτικές»

Η ευρεία διάδοση και εφαρμογή προτύπων στο χώρο των πληροφοριακών συστημάτων έχει πολλαπλή συνεισφορά καθώς συντελεί στη διαλειτουργικότητα ομοειδών πληροφοριακών συστημάτων, στη πιστοποίηση οργανισμών, διαδικασιών, υπηρεσιών, προϊόντων κτλ. Οι πρόσφατες επισκοπήσεις και τεχνικές αναφορές υποδεικνύουν ότι τόσο η αποδοχή διεθνών προτύπων ασφάλειας, όσο και η συμμόρφωση οργανισμών με αυτά, αυξάνεται διαρκώς. Παρόλα αυτά, η πλειοψηφία των οργανισμών εξακολουθεί να μη γνωρίζει τα κυριότερα πρότυπα ασφάλειας ή να μη τα εφαρμόζει στο σύνολό τους. Η παρούσα εργασία έχει ως σκοπό να διευκολύνει την ενημερότητα των επαγγελματιών ασφάλειας για τα διεθνή και

ευρέως διαδεδομένα πρότυπα ασφάλειας, συντελώντας με αυτό τον τρόπο στην υιοθέτησή τους. Η συνεισφορά της εργασίας έγκειται στην πρόταση και αξιοποίηση ενός πλαισίου κατάταξης των προτύπων ασφάλειας, το οποίο περιλαμβάνει τέσσερα επίπεδα. Ο τρόπος με τον οποίο θα μπορούσαν οι επαγγελματίες ασφάλειας να αξιοποιήσουν το παρεχόμενο πλαίσιο προκειμένου να ενημερωθούν και να αναζητήσουν το κατάλληλο κάθε φορά πρότυπο ασφάλειας, παρουσιάζεται μέσα από μία μελέτη περίπτωσης ενός πληροφοριακού συστήματος μισθοδοσίας και συντάξεων.

- J.6 *Tsohou A., Lambrinouidakis C., Kokolakis S., Gritzalis S., “The Importance of Context Dependant Privacy Requirements and Perceptions to the Design of Privacy Aware Systems”, The European Journal of the Informatics Professional (UPGrade), Vol. XI, Issue 1, February 2010, pp. 32-37.*

Τίτλος: «Η Σημασία των Εξαρτώμενων από το Πλαίσιο Απαιτήσεων και Αντιλήψεων Ιδιωτικότητας για το Σχεδιασμό Συστημάτων που Διαφυλάσσουν την Ιδιωτικότητα»

Το ζήτημα της προστασίας της ιδιωτικότητας των πληροφοριών αντιμετωπίζεται θεσμικά σήμερα τόσο σε επίπεδο Ευρωπαϊκής όσο και Εθνικής νομοθεσίας. Παρόλα αυτά, δεν είναι δυνατό να επιτευχθεί ικανοποιητική προστασία της ιδιωτικότητας των χρηστών πληροφοριακών συστημάτων, χωρίς την ύπαρξη τεχνικών έκφρασης των απαιτήσεων ιδιωτικότητας και την εφαρμογή μεθόδων αποτίμησης ιδιωτικότητας που θα προσδιορίζουν τα απαιτούμενα επίπεδα ιδιωτικότητας και τα εναλλακτικά μέτρα ασφάλειας για την επίτευξη αυτών. Στην παρούσα εργασία αξιοποιούμε την υπάρχουσα γνώση από τη διοίκηση ασφάλειας με σκοπό να αναδειχθούν τα ζητήματα που πρέπει να διερευνηθούν προκειμένου να επιτευχθεί η διοίκηση της ιδιωτικότητας, ώστε να είναι εφικτό να επιλέγονται τεκμηριωμένα τεχνολογίες προστασίας της ιδιωτικότητας λαμβάνοντας υπόψη τις ιδιαιτερότητες και απαιτήσεις του συγκεκριμένου συστήματος και πλαισίου.

- J.5 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., "Aligning Security Awareness with Information Systems Security Management", Journal of Information System Security – Vol. 6, No. 1, 2010, pp. 36-54. (Republication of C.4)*

Τίτλος: «Ευθυγράμμιση της Ενημερότητας Ασφάλειας με τη Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων»

Στην παρούσα εργασία διερευνάται ο τρόπος με τον οποίο η διαδικασία της ενημερότητας ασφάλειας συνδέεται με το ευρύτερο πλαίσιο διοίκησης ασφάλειας πληροφοριακών

συστημάτων (ΠΣ) το οποίο εξυπηρετεί. Μέχρι σήμερα, η διαμόρφωση πρωτοβουλιών ενημερότητας ασφάλειας αγνοεί την ιδιαίτερα σημαντική συσχέτιση με το συνολικό πλαίσιο διοίκησης ασφάλειας, και αντίστροφα. Σε αυτή την εργασία τεκμηριώνεται πώς οι δύο διεργασίες μπορούν να ευθυγραμμιστούν, ώστε να διασφαλίζεται ότι οι δραστηριότητες ενημερότητας εξυπηρετούν τη στρατηγική διοίκησης ασφάλειας, αλλά και ότι η διοίκηση ασφάλειας αξιοποιεί τα οφέλη από τις ενέργειες ενημερότητας. Για αυτό το σκοπό πραγματοποιείται ανάλυση των δύο διεργασιών με χρήση ενός πλαισίου ανάλυσης οργανωσιακών διαδικασιών και στη συνέχεια με τη ανάλυση των αναδεικνυόμενων αλληλεπιδράσεων. Η αναγνώριση των αλληλεπιδράσεων αυτών έχει ως αποτέλεσμα να καθίσταται δυνατή η τοποθέτηση της ενημερότητας ασφάλειας στο ευρύτερο πλαίσιο διοίκησης ασφάλειας ΠΣ, σε αντίθεση με την αντιμετώπισή της ως έναν μεμονωμένο μηχανισμό ασφάλειας.

- J.4 *Rizomiliotis P., Tsohou A., Lambrinouidakis C., Gritzalis S., "Security and Privacy Issues in Bipolar Disorder Research", The Journal on Information Technology in Healthcare, Vo. 7, No. 4, 2009, HL7 Ramius Corp. (Republication of C.2)*

Τίτλος: «Ζητήματα Ασφάλειας και Ιδιωτικότητας στην Έρευνα Διπολικής Διαταραχής»

Παρά το γεγονός ότι υπάρχει ανάγκη έρευνας στο χώρο των ψυχικών ασθενειών, η σχετική έρευνα παρεμποδίζεται από τα ζητήματα εμπιστευτικότητας και προστασίας της ιδιωτικότητας που αφορούν τους ιατρικούς φακέλους. Η συγκέντρωση του ιατρικού ιστορικού ασθενών που πάσχουν από την ίδια ασθένεια σε κεντρικές βάσεις δεδομένων, όπου μπορούν να εφαρμοστούν προηγμένες τεχνικές εξόρυξης γνώσης θα ήταν ιδιαίτερα πολύτιμες για τους ερευνητές. Η μεγαλύτερη πρόκληση είναι η ανωνυμοποίηση των δεδομένων, ώστε να ικανοποιούνται οι νομικές και ηθικές απαιτήσεις, ενώ παράλληλα να διατηρούνται οι κρίσιμες ιατρικές πληροφορίες. Στην παρούσα εργασία προτείνεται ένα μοντέλο δημιουργίας κεντρικού αποθετηρίου ανωνυμοποιημένων δεδομένων ασθενών που πάσχουν από διπολική διαταραχή. Η γνώση αυτή τροφοδοτεί ένα ευφύες σύστημα που διευκολύνει και καθοδηγεί τους κλινικούς γιατρούς στη διαχείριση ασθενών. Οι απαιτήσεις ασφάλειας ικανοποιούνται από την εφαρμογή ελέγχου πρόσβασης με μηχανισμούς ελέγχου πρόσβασης βάσει ρόλων (Role Based Access Control).

- J.3 *Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., "Investigating information security*

awareness: research and practice gaps”, Information Security Journal: A Global Perspective, Vol.17, No. 5-6, pp. 207-227, 2008, Taylor and Francis.

Τίτλος: «Διερευνώντας την Ενημερότητα Ασφάλειας Πληροφοριών: Κενά Έρευνας και Πρακτικής»

Η εργασία αυτή παρέχει μία διερευνητική επισκόπηση που στοχεύει αφενός στην αναγνώριση πρότυπων και τάσεων στον τρόπο με τον οποίο η επαγγελματική και η ακαδημαϊκή κοινότητα προσεγγίζουν το ζήτημα της ενημερότητας ασφάλειας, και αφετέρου, στην κατανόηση των αιτιών για τις οποίες η πρακτική της ενημερότητας ασφάλειας παραμένει άλυτο πρόβλημα. Η μέθοδος που εφαρμόστηκε είναι ανάλυση επιλεγμένων δημοσιευμένων εργασιών (επιστημονικά άρθρα, επισκοπήσεις, πρότυπα και τεχνικές αναφορές) με ανοικτή κωδικοποίηση (open coding). Η ανάλυση αυτή οδήγησε σε ένα σχήμα ταξινόμησης έξι κατηγοριών ανοικτών θεμάτων (π.χ. σύγχυση ορολογίας) και οι επιλεγμένες εργασίες κατηγοριοποιήθηκαν σύμφωνα με αυτό το σχήμα. Η παρούσα εργασία οδηγεί στην ανάδειξη ασαφών ζητημάτων των υπάρχουσών προσεγγίσεων ενημερότητας ασφάλειας, ενώ η προτεινόμενη ταξινόμηση παρέχει ένα οδηγό προς τους ερευνητές και επαγγελματίες ασφάλειας για το σχεδιασμό και τη μελέτη ερευνητικών ή εφαρμοσμένων προσεγγίσεων ενημερότητας ασφάλειας πληροφοριακών συστημάτων.

- J.2 *Tsohou A., Kokolakis S., Karyda M., Kiountouzis E., "Process-Variance Models in Information Security Awareness Research", Information Management and Computer Security, Vol.16, No. 3, pp. 271 – 287, 2008, Emerald.*

Τίτλος: «Μοντέλα Μεταβλητότητας και Μοντέλα Διεργασιών της Έρευνας Ενημερότητας Ασφάλειας Πληροφοριών»

Σκοπός της εργασίας είναι να μελετηθεί ο τρόπος με τον οποίο οι μελετητές ασφάλειας πληροφοριακών συστημάτων (ΠΣ) έχουν προσεγγίσει το ζήτημα της ενημερότητας ασφάλειας πληροφοριών και να εξεταστεί κατά πόσο οι προσεγγίσεις αυτές είναι συμβατές με την οργανωσιακή θεωρία και τις προσεγγίσεις μελέτης οργανωσιακών διεργασιών στο χώρο των ΠΣ. Για αυτό το σκοπό πραγματοποιήθηκε ανάλυση επιλεγμένων δημοσιευμένων εργασιών (επιστημονικά άρθρα, επισκοπήσεις, πρότυπα και τεχνικές αναφορές) με ανοικτή κωδικοποίηση (open coding). Η ανάλυση είχε ως αποτέλεσμα την κατηγοριοποίηση των επιλεγμένων δημοσιευμένων εργασιών σύμφωνα με προτεινόμενη τυπολογία. Τα αποτελέσματα της εργασίας διευκολύνουν τους ερευνητές και επαγγελματίες ασφάλειας ΠΣ

ώστε να διακρίνουν και να εφαρμόζουν κατάλληλα μοντέλα έρευνας στο σχεδιασμό πρωτοβουλιών και τη μελέτη ζητημάτων ενημερότητας ασφάλειας ΠΣ.

- J.1 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., "Formulating Information Systems Risk Management Strategies through Cultural Theory", Information Management and Computer Security, Vol. 14, No. 3, pp. 198-217, 2006, Emerald.*

Τίτλος: «Διαμορφώνοντας Στρατηγικές Διαχείρισης Επικινδυνότητας Πληροφοριακών Συστημάτων Εφαρμόζοντας το Πολιτισμικό Πρότυπο»

Σκοπός της παρούσας εργασίας είναι η διερεύνηση της εφαρμογής του Πολιτισμικού Προτύπου ως εργαλείο αναγνώρισης προτύπων στις αντιλήψεις επικινδυνότητας των εμπλεκόμενων στην ασφάλεια πληροφοριών και της επίδρασής τους στη διαχείριση επικινδυνότητας πληροφοριακών συστημάτων (ΠΣ). Σύμφωνα με το Πολιτισμικό Πρότυπο οι αντιλήψεις επικινδυνότητας μεταξύ κοινωνικών ομάδων και δομών είναι προβλέψιμη και συσχετίζεται με τον τύπο κοινωνικής οργάνωσης. Η διαχείριση επικινδυνότητας ΠΣ περιλαμβάνει ένα σημαντικό αριθμό δραστηριοτήτων που βασίζονται στον τρόπο με τον οποίο οι εμπλεκόμενοι αντιλαμβάνονται τον κίνδυνο σε σχέση με τα αγαθά του ΠΣ. Επομένως, στην παρούσα εργασία εξετάζονται οι επιπτώσεις της εφαρμογής του Πολιτισμικού Προτύπου στη διαχείριση ασφάλειας ΠΣ ως εργαλείο των ειδικών ασφάλειας για τη διαχείριση των αντιλήψεων επικινδυνότητας. Η εργασία παρουσιάζει πώς οι διαφορετικοί τύποι μορφών κοινωνικής οργάνωσης επηρεάζουν τη διαχείριση επικινδυνότητας και παρέχει κύρια σημεία που πρέπει να λαμβάνονται υπόψη κατά τη διαμόρφωση στρατηγικών διαχείρισης επικινδυνότητας.

B.3 ΕΡΕΥΝΗΤΙΚΕΣ ΕΡΓΑΣΙΕΣ ΔΗΜΟΣΙΕΥΜΕΝΕΣ ΣΕ ΠΡΑΚΤΙΚΑ ΔΙΕΘΝΩΝ ΕΠΙΣΤΗΜΟΝΙΚΩΝ ΣΥΝΕΔΡΙΩΝ ΜΕΤΑ ΑΠΟ ΚΡΙΣΗ ΠΛΗΡΟΥΣ ΚΕΙΜΕΝΟΥ

- C.22 Gritzalis, A., *Tsohou A.* and Lambrinouidakis C. Transparency Enabling Systems for Open Governance: Their Impact on Citizens' Trust and the Role of Information Privacy, In the Proceedings of the 7th International Conference on eDemocracy, Privacy-Preserving, Secure, Intelligent eGovernment Services, 14 – 15 December 2017, Athens - Greece

Several governments and citizens embrace information systems that are designed to enable transparency of public expenses and discourage corruption in the public sector. The objective of this

paper is to examine the capacity and value of information systems designed to enhance transparency, from a citizens'/users' perspective. Our purpose is to address research questions associated with the actual impact of transparency-enabling systems and openness on citizens' trust and uncertainty towards the governmental policies and actions. We also explored the impact of privacy requirements and personal data protection regulations on the system and citizens' willingness to access public data. To the best of our knowledge, these are largely unexplored issues in the literature. Our study involves the design of a web survey and the execution of an empirical study with citizens who have used such a system in Greece. In particular, we focused our empirical study on the Greek system 'Diavgeia', which is the national transparency and anti-corruption system

- C. 21 Kosyfaki, C., Angelova N., Tsohou A. and Magkos, M. (2017) The Privacy Paradox in the Context of Online Health Data Disclosure by Users, *In the Proceedings of the 14th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS 2017)*, Coimbra, Portugal, September 2017, Springer.

The privacy paradox phenomenon corresponds to the inconsistency between the privacy concerns and the actual behavior of online users [9]. The existence of the phenomenon has been studied in many fields, such as social networks and especially a great variety of forums and online communities [3, 6]. This paper, questions its existence in the context of sensitive data, and more specific in the health data area via a survey which took place in Greece. Given that health-related information are perceived as highly sensitive personal data and are often excluded from discussions and sharing, this research aims to unravel the paradox's existence that leads to the disclosure of health data information during the visit of related online forums and communities, by the users.

- C. 20 Paspatis, I., Tsohou A. and Kokolakis S. (2017), *Mobile Application Privacy Risks: Viber Users' De-Anonymization Using Public Data*, *In the Proceedings of the 11th Mediterranean Conference on Information Systems, Genova, Italy, September 2017, Association for Information Systems (AIS)*.

Mobile application developers define the terms of use for the applications they develop, which users may accept or declined during installation. Application developers on the one hand seek to gain access to as many user information as possible, while users on the other hand seem to lack awareness and comprehension of privacy policies. This allows application developers to store an enormous number of personal data, sometimes even irrelevant to the application's function. It's also common that users choose not to alter the default settings, even when such an option is provided. In combination, the above conditions jeopardize users' rights to privacy. In this research, we examined the Viber application to demonstrate how effortless it is to discover the identity of unknown Viber users. We

chose a pseudorandom sample of 2000 cellular telephone numbers and examined if we could reveal their personal information. We designed an empirical study that compares the reported behavior with the actual behavior of Viber's users. The results of this study show that users' anonymity and privacy is easily deprived and information is exposed to a knowledgeable seeker. We provide guidelines addressed to both mobile application users and developers to increase privacy awareness and prevent privacy violations.

- C.19 Skalkos A., Tsohou A., Karyda M. and Kokolakis S. (2017) Investigating the Values that Drive the Adoption of Anonymity Tools: A Laddering Approach, Research In progress, *The 11th Mediterranean Conference on Information Systems*, Genova, Italy, September 2017

Concerns about privacy and frustration over censorship and content blocking are driving millions to use privacy enhancing products. This research-in-progress focuses on anonymity tools, as a Privacy Enhancing Technology (PET), investigating the values that drive the adoption of anonymity tools by users. We use means-end analysis, a methodology we consider to be appropriate for investigating users' conceptions and incentives for adopting anonymity tools. We also use the laddering technique, a qualitative method based on in-depth interviews, to reveal the chains of attribute-consequence-values of anonymity tools users and to construct a Hierarchical Value Map. The aim of our research is to provide insights and enhance understanding of anonymity tools users' behavior, which we expect to benefit both researchers and software engineers to design platforms that more closely fit users' need.

- C.18 *Diamantopoulou V., Tsohou A., Loukis E. and Gritzalis S. (2017) Does the Development of Information Systems Resources Lead to the Development of Information Security Resources? An Empirical Investigation, In the Proceedings of the 23rd Americas Conference on Information Systems (AMCIS 2017), Boston, USA, August 2017*

Information Systems (IS) are nowadays considered the most important leverage for organizations to operate and gain a competitive advantage. Investments in IS technology, in the recruitment of high qualified IT personnel and the establishment of internal and external robust IT related partnerships are considered determinant factors for business success and continuity. As organizations increasingly rely on IS resources, they face more advanced IS security challenges. This paper explores the relationship between the development of IS resources and security resources; are organizations willing to invest more in IS security resources as they invest more on IS resources? The authors conduct an empirical investigation in organizations located in five Mediterranean countries. The sample includes responses from 61 CEOs, information security managers and IS managers. The results reveal that IS resources

positively affect the IS security resources. The human capital plays the most important role for the adoption of IS security.

- C.17 *Karavaras E., Magkos E. and Tsohou A. (2016) Low User Awareness Against Social Malware: an Empirical Study and Design of a Security Application, In the Proceedings of the 13th European, Mediterranean and Middle Eastern Conference on Information Systems, Krakow, Poland, June 2016*

During the past few years, in harmony with the fast growing rate of user population in Online Social Networks (OSNs), a trend for malware writers has been to take advantage of the social relationships of OSN users, in order to lure them into following malicious URLs that lead to malware infection. One reason for the success of such Social Engineering (SE)-based malware has been the low security awareness of OSN users. Indeed, it can be shown that, on the average, OSN users do not have sufficient knowledge of the malicious link threats they may come up against, and thus are easy victims of SE attacks. In this paper we conduct an empirical investigation which, on the one hand, demonstrates Facebook users' low awareness of malicious link threats, and on the other hand explores the views of OSN users on the desirable properties of a security application that protects them against social malware. Furthermore, we design and describe the architecture of a security application which intends to raise Facebook users' security awareness by informing them about (possibly) malicious posts on their walls before or after they get infected. Our application acts proactively by helping users to not get infected by malicious posts, and reactively by helping the users who got infected to gain an understanding of the threat and become more alerted towards identifying malware links.

- C.16 *Jiang H. and Tsohou A. (2015), The same Antecedents do not fit all activities: an Activity-Specific Model of Personal Internet Use in Workplace, (Research in Progress), In Proceedings of the 23rd European Conference on Information Systems (ECIS 2015), May 2015, Mursten, Germany*

Τίτλος: «Οι ίδιοι Παράγοντες Διαμόρφωσης δεν Ταιριάζουν σε Όλες τις Ενέργειες: Ένα Μοντέλο Εξειδικευμένο Ανά Ενέργεια για την Προσωπική Χρήση του Διαδικτύου στον Εργασιακό Χώρο»

Οι νέες τεχνολογίες με σύνδεση στο Διαδίκτυο, όπως προσωπικοί υπολογιστές, tablets και κινητά τηλέφωνα, χρησιμοποιούνται διαρκώς από τους οργανισμούς. Ταυτόχρονα,

παρατηρείται αύξηση του φαινομένου χρήσης από τους υπαλλήλους ενός οργανισμού των νέων τεχνολογιών για προσωπικούς λόγους εν ώρα εργασίας. Η βιβλιογραφία παρουσιάζει διάφορα μοντέλα ανάλυσης των αιτιών για τους οποίους οι υπάλληλοι πράττουν κατάχρηση των πόρων με αυτό τον τρόπο. Οι έρευνες αυτές αντιμετωπίζουν τη χρήση των νέων τεχνολογιών για προσωπικούς λόγους ως μία ενιαία συμπεριφορά. Παρόλα αυτά υπάρχουν έρευνες που υπονοούν ότι υπάρχουν διάφοροι τύποι συμπεριφοράς που εντάσσονται σε αυτό το πεδίο. Επομένως, είναι περιοριστικό να μελετούμε ως ένα ενιαίο φαινόμενο το πρόβλημα αυτό και τις αιτίες του. Ως ένα πρώτο βήμα την αντιμετώπιση αυτού του ερευνητικού κενού, η εργασία αυτή διαχωρίζει τρεις κατηγορίες χρήσης των νέων τεχνολογιών για προσωπικούς λόγους: χρήση ηλεκτρονικού ταχυδρομείου, πλοήγηση στο Διαδίκτυο και οικονομικές συναλλαγές. Εξετάζουμε διαφορετικές αιτίες για κάθε μία από τις τρεις κατηγορίες. Η εργασία συνεισφέρει στην έρευνα αναδεικνύοντας την αναγκαιότητα να εξεταστεί σε βάθος το φαινόμενο διακρίνοντας διαφορετικούς τύπους χρήσης.

- C.15 *Koufi V., Tsohou A., Malamateniou F. and Vassilacopoulos G., (2014), A Framework for Privacy-Preserving Access Control to Cloud Process-based EHR Systems, 25th European Medical Informatics Conference, August 2014, Istanbul, Turkey.*

Τίτλος: «Ένα Πλαίσιο για την Έλεγχο Πρόσβασης που Προστατεύει την Ιδιωτικότητα σε Συστήματα Νεφρολογιστικής Ηλεκτρονικού Φακέλου Υγείας»

Παρά το γεγονός ότι η προσωποποιημένη ιατρική μπορεί να βελτιστοποιήσει την εύρεση, ανάπτυξη και εφαρμογή θεραπευτικών δράσεων, δεν έχει πλήρως αξιοποιηθεί από τις υπηρεσίες υγείας προς ασθενείς. Όταν ο ηλεκτρονικός φάκελος υγείας ενσωματωθεί με δεδομένα από άλλες πηγές, όπως κοινωνική πρόνοια, προσωπικό φάκελο υγείας και γενικές πληροφορίες, μπορεί να αποκτήσει κεντρικό ρόλο στην προσωποποιημένη υγειονομική περίθαλψη. Επομένως, μία νέα γενιά ηλεκτρονικού φακέλου υγείας θα αναδυθεί η οποία όχι μόνο θα υποστηρίζει τους επαγγελματίες υγείας να λαμβάνουν κατάλληλα πληροφορημένες αποφάσεις, αλλά επίσης μπορεί να υποστηρίξει την καινοτόμα ανακάλυψη συσχετίσεων ανάμεσα σε γενετικά, κλιματολογικά, διαδικαστικά στοιχεία. Παρόλα, υπάρχει ένα πλήθος από νομικά, ηθικά και τεχνικά αίτια που παρεμποδίζουν την υλοποίηση αυτού του ηλεκτρονικού φακέλου υγείας, εξ' αιτίας των πιθανών παραβιάσεων ασφάλειας πληροφοριών και της ιδιωτικότητας. Σε αυτή την εργασία παρουσιάζουμε ένα μοντέλο συμβατό με τη HIPAA το οποίο ενεργοποιεί έλεγχο πρόσβασης στην επόμενη γενιά ηλεκτρονικού φακέλου

υγείας διατηρώντας την ιδιωτικότητα.

- C.14 *Jiang H. and Tsohou A. Expressive Or Instrumental: A Dual-Perspective Model Of Personal Web Usage At Workplace (Research in Progress) In Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), June 2014, Tel Aviv, Israel*

Τίτλος: «Η Πλευρά της Έκφρασης και του Σκοπού: Ένα Δυϊκό Μοντέλο για την Επεξήγηση της Προσωπικής Χρήσης του Διαδικτύου στον Εργασιακό Χώρο»

Η χρήση κινητών συσκευών, όπως κινητά τηλέφωνα και tablets, κατέχουν σήμερα εξαιρετικά σημαντικό ρόλο σε προσωπικούς και επαγγελματικούς τομείς. Εν τω μεταξύ, οι τεχνολογικές εξελίξεις καθιστούν ολοένα και πιο δύσκολη τη διάκριση ανάμεσα στις εργασιακές και τις μη εργασιακές δραστηριότητες. Καθώς οι κινητές συσκευές και το Διαδίκτυο εντάσσονται όλο και περισσότερο στον εργασιακό χώρο, οι υπάλληλα συχνά πραγματοποιούν ενέργειες στο Διαδίκτυο που αφορούν προσωπικές υποθέσεις, εν ώρα εργασίας και από τον εργασιακό χώρο, αξιοποιώντας μάλιστα τεχνολογικούς πόρους του οργανισμού. Οι έρευνες έχουν αναγνωρίσει πληθώρα από κίνητρα που εξηγούν αυτή τη συμπεριφορά, από διαφορετικές οπτικές. Μέσω ανάλυσης της βιβλιογραφίας, προτείνουμε ένα δυϊκό μοντέλο για τη συμπεριφορά αυτή και εξετάζουμε τους παράγοντες διαμόρφωσης, τους οποίους διακρίνουμε σε δύο κατηγορίες: τους παράγοντες έκφρασης και τους παράγοντες σκοπού. Στη συνέχεια, αναπτύσσουμε ένα δυϊκό ερευνητικό μοντέλο συνδυάζοντας τις δύο κατηγορίες και τις αλληλοεπιδράσεις τους. Συγκεκριμένα, αξιοποιώντας τη θεωρία ελέγχου-ζήτησης εργασίας (job demand-control theory) αναγνωρίζουμε ένα νέο παράγοντα διαμόρφωσης που εξηγεί την πλευρά έκφρασης της συμπεριφοράς, την επαγγελματική εξουθένωση. Επίσης, αναγνωρίζουμε ένα νέο παράγοντα διαμόρφωσης που εξηγεί την πλευρά σκοπού της συμπεριφοράς, το εκτιμώμενο όφελος. Το μοντέλο δίνει νέα οπτική στην έρευνα γύρω από τη συμπεριφορά προσωπικής χρήσης του Διαδικτύου στον εργασιακό χώρο, μέσω της πρότασης αναγνώρισης της διττής φύσης της, δίνοντας μία ευκαιρία κατανόησης των διαφορετικών εναλλακτικών μοντέλων που υπάρχουν στη βιβλιογραφία και επιτρέποντας το συνδυασμό τους σε μελλοντική έρευνα.

- C.13 *Jiang H. and Tsohou A. The Dual Nature of Personal Web Usage At Workplace: Impacts, Antecedents And Regulating Policies, In Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), June 2014, Tel Aviv, Israel*

Τίτλος: «Η Διττή Φύση της Προσωπικής Χρήσης του Διαδικτύου στον Εργασιακό Χώρο:

Επιπτώσεις, Παράγοντες Διαμόρφωσης και Πολιτικές Ασφάλειας»

Η χρήση κινητών συσκευών, όπως κινητά τηλέφωνα και tablets, κατέχουν σήμερα εξαιρετικά σημαντικό ρόλο σε προσωπικούς και επαγγελματικούς τομείς. Εν τω μεταξύ, οι τεχνολογικές εξελίξεις καθιστούν ολοένα και πιο δύσκολη τη διάκριση ανάμεσα στις εργασιακές και τις μη εργασιακές δραστηριότητες. Υπάρχουν αντικρουόμενες απόψεις στη βιβλιογραφία σχετικά με τους παράγοντες διαμόρφωσης, τις επιπτώσεις και τις πολιτικές ασφάλειας που περιορίζουν της προσωπικής χρήσης του Διαδικτύου στον εργασιακό χώρο. Σε αυτή την εργασία ισχυριζόμαστε ότι για να κατανοήσουμε το φαινόμενο θα πρέπει να αναλύσουμε περισσότερο τη συμπεριφορά αυτή και να κατανοήσουμε τη φύση της. Μέσω ανάλυσης της σχετικής βιβλιογραφίας προτείνουμε ότι η συμπεριφορά αυτή έχει διττή φύση η οποία συνδέεται με διαφορετικούς παράγοντες διαμόρφωσης, επιπτώσεις και πολιτικές περιορισμού. Αναφορικά με τους παράγοντες διαμόρφωσης η συμπεριφορά αυτή αποτελεί ταυτόχρονα ένα μέσο για να εκφράσουν αρνητικά συναισθήματα σε σχέση με τον οργανισμό και ένα μέσο σκοπού για την επίτευξη θετικών λειτουργιών χρησιμοποιώντας το Διαδίκτυο. Σε σχέση με τις επιπτώσεις αναγνωρίζουμε ότι η συμπεριφορά αυτή μπορεί να επιφέρει τόσο θετικές επιπτώσεις στους οργανισμούς όσο και αρνητικές. Για τις πολιτικές ασφάλειας, διακρίνουμε ότι διαφορετικές πολιτικές είναι κατάλληλες ανάλογα τον οργανισμό. Αυτή η διττή φύση της συμπεριφορά προσωπικής χρήσης του Διαδικτύου στον εργασιακό χώρο προσφέρει νέα οπτική στο φαινόμενο για δύο λόγους. Πρώτον διευκολύνει την ενοποίηση των αντικρουόμενων ερευνών στη βιβλιογραφία και δεύτερον παρέχει καθοδήγηση για μελλοντική έρευνα.

- C.12 *Oh J., Lee H. and Tsohou A. Relational Versus Structural Embeddedness in IT Outsourcing Networks: The Role Of Requirement Unpredictability And Measurement Difficulty, 17th Pacific Asia Conference on Information Systems (PACIS 2013), June 2013, Jeju Island, Korea*

Τίτλος: «Η Σχετική Έναντι στη Δομική Ενσωμάτωση σε Δίκτυα Συνεργατών Εξωτερικής Ανάθεσης Τεχνολογιών Πληροφορικής: Ο ρόλος της Προβλεψιμότητας και της Δυσκολίας Μέτρησης»

Η σχετική και η δομική ενσωμάτωση κατέχουν σημαντικό ρόλο στο πλαίσιο της ανάθεσης εργασιών πληροφοριακών συστημάτων σε τρίτους φορείς. Παρόλα αυτά, δεν υπάρχει σαφής καθοδήγηση για το ποιος από τους δύο τύπους ενσωμάτωσης είναι πλέον κατάλληλος προκειμένου να αποτραπούν συμπεριφορές κερδοσκοπίας και να επιτευχθεί μακροπρόθεσμη επίδοση όταν υπάρχει αβεβαιότητα και ένα μεγάλο εύρος ανάπτυξης προϊόντων και

συστημάτων πληροφορικής που έχουν ανατεθεί σε τρίτους. Προκειμένου να απαντήσουμε σε αυτό το ερώτημα, δημιουργούμε ένα εικονικό περιβάλλον που προσομοιάζει το δίκτυο συνεργατών μία τρίτης ανάθεσης, όπου οι εταιρείες παίρνουν τον έλεγχο επιλογής συνεργατών με σχετική και με δομική ενσωμάτωση αντίστοιχα. Οι συνεργάτες ανταγωνίζονται μεταξύ τους με στόχο τη μεγιστοποίηση των μακροπρόθεσμων κερδών. Τα αποτελέσματα της προσομοίωσης δείχνουν τα πλεονεκτήματα του κάθε τύπου ενσωμάτωσης και ότι υπερέχουν κάθε ένας ανάλογα με τα επίπεδα αβεβαιότητας. Επομένως, η έρευνα παρέχει καλύτερη κατανόηση των συνθηκών υπεροχής του κάθε τύπου και παρέχει στην ανώτερη διοίκηση καθοδήγηση για να επιλέξει ανάμεσά τους.

- C.11 *Tsohou A., Al-Yafi K., Lee H., “Evaluating M-Government Applications: An Elaboration Likelihood Model Framework”, Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS), (Eds. Ghoneim A., Klischewski R., Schrödl H., Muhammed K.) 2012, 7-8 June, Munich, Germany*

Τίτλος: «Αξιολογώντας Εφαρμογές κινητής Διακυβέρνησης: Ένα πλαίσιο με βάση το Elaboration Likelihood Model»

Οι εφαρμογές και υπηρεσίες κινητής διακυβέρνησης (m-government) αναφέρονται σε υπηρεσίες που είναι διαθέσιμες μέσω κινητών συσκευών συνδεδεμένων στο Διαδίκτυο και είναι προσπελάσιμες οποιαδήποτε ώρα και από οποιαδήποτε τοποθεσία. Η κινητή διακυβέρνηση και η κινητή συμμετοχή των πολιτών είναι νέες έννοιες ενός αναπτυσσόμενου πεδίου της δημόσιας διακυβέρνησης και παρέχεται μέσω ηλεκτρονικών υπηρεσιών προσβάσιμων από κινητές συσκευές. Σε αυτή την εργασία παρέχουμε ένα πλαίσιο αξιολόγησης των εργαλείων κινητής διακυβέρνησης. Το πλαίσιο αξιολόγησης βασίζεται στην υπόθεση ότι τα εργαλεία κινητής διακυβέρνησης δεν παρέχουν μόνο μία εναλλακτική μέθοδο πρόσβασης στις δημόσιες δράσεις, αλλά στοχεύει και στην παροχή κινήτρων στους πολίτες για την αύξηση της συμμετοχής τους στις διαδικασίες διαμόρφωσης δημόσιων πολιτικών. Η μέθοδος αξιολόγησης βασίζεται στο μοντέλο Elaboration Likelihood Model. Η καινοτομία της εργασίας συνίσταται α) στην ικανότητα της να αποτυπώνει την πραγματική χρήση των εργαλείων από τους χρήστες και όχι την πρόθεση χρήσης, β) στη δυνατότητα που φέρει να αποτιμά τις ικανότητες κινητοποίησης και πειθούς του συστήματος.

- C.10 *Tsohou A., Lee H., Zahir I., Weerakkody V., Osman I., Latif A., Medeni T., “Evaluating E-Government Services From A Citizens’ Perspective: A Reference Process Model”,*

Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS), (Eds. Ghoneim A., Klischewski R., Schrödl H., Muhammed K.), 7-8 June, 2012, Munich, Germany

Τίτλος: «Αξιολογώντας Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης με Πολιτο-κεντρική Προσέγγιση: Ένα Διεργασιακό Μοντέλο Αναφοράς»

Η αξιολόγηση και βελτιστοποίηση των υπηρεσιών ηλεκτρονικής διακυβέρνησης είναι απαραίτητη για τις κυβερνήσεις, ιδιαίτερα λόγω της δυνατότητας που φέρουν για την μεταρρύθμιση της δημόσιας διοίκησης. Οι υπάρχουσες προσεγγίσεις αξιολόγησης δεν συμπεριλαμβάνουν μετρικές που αντανακλούν την ικανοποίηση των πολιτών. Η βιβλιογραφία από την άλλη μεριά περιλαμβάνει διάφορα μοντέλα και τεχνικές για την αξιολόγηση της ικανοποίησης των πολιτών. Παρόλα αυτά, η βιβλιογραφία στερείται ενός μοντέλου αναφοράς για την επανα-χρησιμοποίηση πρακτικών αξιολόγησης ηλεκτρονικών υπηρεσιών διακυβέρνησης με συμπερίληψη της ικανοποίησης των πολιτών. Σε αυτή την εργασία, αξιοποιούμε την προσέγγιση αξιολόγησης που αναπτύχθηκε στο πλαίσιο του Κοινοτικού Προγράμματος CEES και προτείνουμε ένα μοντέλο αναφοράς που ενσωματώνει τη δυνατότητα επανα-χρησιμοποίησης πρακτικών ηλεκτρονικής διακυβέρνησης με πολιτο-κεντρική προσέγγιση. Η καινοτομία της εργασίας έγκειται στη χρήση της τεχνικής ανάλυσης φακέλου δεδομένων για την αξιολόγηση των ηλεκτρονικών υπηρεσιών προς την αναγνώριση σημείων στρατηγικής βελτίωσης των υπηρεσιών.

- C.9 *El-Haddadeh R., Tsohou A., Karyda M., “Analyzing Implementation Challenges for information Security Awareness initiatives in E-government”, Proceedings of the ECIS 2012 20th European Conference on Information Systems, (Eds. Janssen M, Weerakkody V, Dwivedi Y), June 2012, Barcelona, Spain.*

Τίτλος: «Αναλύοντας τις Προκλήσεις Υλοποίησης Δράσεων Ενημερότητας Ασφάλειας Πληροφοριών για την Ηλεκτρονική Διακυβέρνηση»

Με την ευρεία υιοθέτηση υπηρεσιών ηλεκτρονικής διακυβέρνησης έχει δημιουργηθεί η ανάγκη αδιάκοπης ροής δεδομένων μεταξύ των φορέων του δημοσίου τομέα, διατηρώντας παράλληλα την ακεραιότητα, εμπιστευτικότητα και ακεραιότητα των δεδομένων αυτών. Οι κυβερνήσεις έχουν θέσει σε ισχύ διάφορα κίνητρα και προγράμματα, συμπεριλαμβανομένων προγραμμάτων ενημερότητας, με σκοπό την ενίσχυση της κατανόησης για την προστασία της ασφάλειας πληροφοριών και της ιδιωτικότητας από τους υπαλλήλους των δημοσίων φορέων.

Παρόλα αυτά, η υλοποίηση τέτοιων δράσεων ενημερότητας είναι πολλές φορές συνυφασμένη με ένα πλήθος από προκλήσεις. Η εργασία αυτή προσφέρει μία κατανόηση των προκλήσεων προς την επιτυχή υλοποίηση προγραμμάτων ενημερότητας ασφάλειας στον δημόσιο τομέα σε σχέση με τις ηλεκτρονικές υπηρεσίες. Το εννοιολογικό πλαίσιο που αναπτύσσεται περιλαμβάνει πολιτικές, κοινωνικές, οργανωσιακές και τεχνολογικές προκλήσεις. Η εργασία περιλαμβάνει εμπειρική έρευνα μέσω μελέτης περίπτωσης σε ένα δημόσιο οργανισμό στην Ελλάδα. Ενώ τα αποτελέσματα της εμπειρικής έρευνας επιβεβαιώνουν το ρόλο των προκλήσεων που αναγνωρίστηκαν, παράλληλα αναγνωρίζεται μέσω της έρευνας ότι οι συμμετέχοντες στο σχεδιασμό των προγραμμάτων ενημερότητας επιδιώκουν συχνά διαφορετικούς στόχους ασφάλειας και ιδιωτικότητας, το οποίο συντελεί σε αύξηση της πολυπλοκότητας στον οργανισμό.

- C.8 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., “Analyzing Information Security Awareness through Networks of Association”, 7th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2010), September 2010, Bilbao, Spain*

Τίτλος: «Αναλύοντας την Ενημερότητα Ασφάλειας Πληροφοριών αξιοποιώντας Δίκτυα Σύμπραξης»

Η ενημερότητα ασφάλειας πληροφοριών είναι μία διαρκής προσπάθεια εστίασης του ενδιαφέροντος στην ασφάλεια πληροφοριών και τη σημασία της, με σκοπό την ενεργοποίηση συμπεριφορών που ωφελούν την ασφάλεια. Παρά το αυξημένο ενδιαφέρον των ερευνητών στο πεδίο της ενημερότητας ασφάλειας και τις διαρκείς προειδοποιήσεις των διεθνών επισκοπήσεων ασφάλειας για τη σημασία της, η ενημερότητα ασφάλειας παραμένει ως ένα κρίσιμο ζήτημα της ασφάλειας πληροφοριών. Οι υπάρχουσες προσεγγίσεις ενημερότητας ασφάλειας προτείνουν τεχνικές και μεθόδους προώθησης της ασφάλειας, χωρίς όμως να στηρίζονται σε κάποιο θεωρητικό πλαίσιο, και μάλιστα ανεξάρτητα από το συνολικό πλαίσιο διοίκησης ασφάλειας πληροφοριών. Ο σκοπός της παρούσας εργασίας είναι να προτείνει ένα θεωρητικό και μεθοδολογικό πλαίσιο που θα διευκολύνει την ανάλυση και κατανόηση των ζητημάτων που εμπλέκονται στις δραστηριότητες ενημερότητας ασφάλειας, ώστε να υποστηριχθεί η διοίκηση ασφάλειας ενός οργανισμού.

- C.7 *Evans R., Tsohou A., Tryfonas T., Morgan T., “Architecting Secure Systems with the ISO standards 26702 and 27001”, 5th IEEE International Conference on Systems of Systems Engineering (SoSE 2010), June 2010, Loughborough, UK, IEEE Computer Society Press*

Τίτλος: «Σχεδιάζοντας Ασφαλή Συστήματα με τα πρότυπα ISO 26702 και ISO 27001»

Οι σχεδιαστές συστημάτων βρίσκονται αντιμέτωποι με τις ταχείες τεχνολογικές εξελίξεις, τις πολύπλοκες συμβατικές σχέσεις, τις αναδυόμενες απειλές και απαιτήσεις ασφάλειας, τις ανησυχίες για τη βιωσιμότητα των προγραμμάτων τους κτλ. Σε αυτό το πλαίσιο, τα πληροφοριακά συστήματα εκτίθενται σε υψηλούς κινδύνους, ενώ τα πρόσφατα στοιχεία περιστατικών αποτυχίας συντελούν στην απαίτηση έμφασης στην ασφάλεια. Παρόλα αυτά είναι μη εφικτό οι προγραμματιστές συστημάτων να εξειδικευτούν σε όλα τα πεδία ενδιαφέροντος προκειμένου να αντιμετωπίσουν με επιτυχία τα ζητήματα αυτά. Επομένως, ο σχεδιασμός των συστημάτων είναι απαραίτητο να λαμβάνει υπόψη τις καλές πρακτικές και την υπάρχουσα σχετική γνώση. Όταν αυτή η γνώση ενσωματώνεται σε καθιερωμένα και ευρέως αποδεκτά πρότυπα, δημιουργείται όχι μόνο η ευκαιρία να αξιοποιηθεί το ώριμο περιεχόμενό τους, αλλά και να αξιοποιηθούν τα πλεονεκτήματα συμμόρφωσης, ολοκλήρωσης και ανταγωνιστικού πλεονεκτήματος που παρέχει η προτυποποίηση. Για αυτό το σκοπό, στην παρούσα εργασία διερευνάται η αξιοποίηση δύο ευρέως αποδεκτών προτύπων: η σειρά ISO 27000 και το ISO/IEC 26702, ως εργαλεία που θα βοηθήσουν το σχεδιασμό ασφαλών συστημάτων.

- C.6 Vrakas N., Kalloniatis C., Tsohou A., Lambrinouidakis C., “Privacy Requirements Engineering for Trustworthy e-Government Services”, 3rd International Conference on Trust and Trustworthy Computing (TRUST 2010), June 2010, Berlin, Germany, Lecture Notes in Computer Science LNCS, Springer.

Τίτλος: «Ανάλυση και Σχεδίαση Απαιτήσεων Ιδιωτικότητας για Έμπιστες Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης»

Πολλές έρευνες στο χώρο των πληροφοριακών συστημάτων έχουν εφαρμόσει θεωρίες αποδοχής για την εξέταση ζητημάτων αποδοχής ηλεκτρονικών υπηρεσιών από τους χρήστες πληροφοριακών συστημάτων. Η εφαρμογή αυτών των θεωριών στο πεδίο της ηλεκτρονικής διακυβέρνησης έχει δείξει ότι η εμπιστοσύνη αποτελεί προαπαιτούμενο για την αποδοχή και χρήση των συστημάτων ηλεκτρονικής διακυβέρνησης. Παράλληλα, τα ζητήματα και οι ανησυχίες ιδιωτικότητας αποτελούν την κύρια προϋπόθεση για τη πρόθεση χρήσης των συστημάτων ηλεκτρονικής διακυβέρνησης από τους χρήστες. Επομένως, πληροφοριακά συστήματα που δε διαφυλάσσουν την ιδιωτικότητα δεν γίνονται έμπιστα από τους χρήστες με αποτέλεσμα να μη τα αποδέχονται. Σήμερα υπάρχουν πολλές κακόβουλες επιθέσεις που

μπορεί να παραβιάσουν την εμπιστευτικότητα προσωπικών δεδομένων και να διακυβευτεί η εμπιστοσύνη προς το σύστημα. Ο τυπικός τρόπος για την αποτροπή τέτοιων επιθέσεων είναι η εφαρμογή τεχνολογιών προστασίας της ιδιωτικότητας. Παρόλα, η εφαρμογή των τεχνολογιών ενίσχυσης της ιδιωτικότητας εφαρμόζονται σήμερα αυθαίρετα και μη λαμβάνοντας υπόψη τις απαιτήσεις του εκάστοτε οργανωσιακού πλαισίου στο οποίο λειτουργεί ή θα λειτουργεί το σύστημα. Στην παρούσα εργασία ισχυριζόμαστε ότι είναι απαραίτητο να αναπτυχθούν μέθοδοι ανάλυσης και σχεδίασης απαιτήσεων ιδιωτικότητας προκειμένου να ανιχνεύονται οι εξαρτώμενες από το πλαίσιο απαιτήσεις ιδιωτικότητας και να επιλέγονται τα κατάλληλα τεχνικά, οργανωσιακά και διαδικαστικά αντίμετρα για την υλοποίηση συστημάτων ηλεκτρονικής διακυβέρνησης που διαφυλάσσουν την ιδιωτικότητα που θα προσφέρουν ηλεκτρονικές υπηρεσίες που εμπιστεύονται οι χρήστες.

- C.5 *Tsohou A., Kokolakis S., Lambrinouidakis C., Gritzalis S., "Unifying ISO Security Standards Practices into a Single Security Framework", 12th Annual IFIP Workshop on Information Security Management, N.Clarke, S. Furnell (Eds.), May 2010, Port Elizabeth, South Africa, Emerald*

Τίτλος: «Ενοποιώντας τα Διεθνή Πρότυπα Ασφάλειας (ISO) σε ένα Ενιαίο Πλαίσιο Ασφάλειας»

Στο χώρο των πληροφοριακών συστημάτων η συμμόρφωση με πρότυπα είναι ιδιαίτερα σημαντική για ποικίλους λόγους, μεταξύ των οποίων είναι η διαλειτουργικότητα, η πιστοποίηση κτλ. Ενώ οι πρόσφατες επισκοπήσεις υποδεικνύουν ότι η αποδοχή διεθνών προτύπων ασφάλειας αυξάνεται και ότι οι οργανισμοί συμμορφώνονται με αυτά διαρκώς αυξάνεται, παρόλα αυτά η πλειοψηφία των οργανισμών εξακολουθεί να μη γνωρίζει τα κυριότερα πρότυπα ασφάλειας ή να μη εφαρμόζει στο σύνολό τους. Η παρούσα εργασία έχει ως σκοπό να διευκολύνει την ενημερότητα των επαγγελματιών ασφάλειας για τα διεθνή πρότυπα ασφάλειας και να συνεισφέρει στην εφαρμογή τους μέσα από ένα πλαίσιο ασφάλειας που προτείνεται. Το προτεινόμενο πλαίσιο ασφάλειας περιλαμβάνει τέσσερα επίπεδα. Για την επεξήγηση των διαφορετικών επιπέδων και την παρουσίαση της εφαρμοσιμότητάς του χρησιμοποιούμε ως μελέτη περίπτωσης ένα πληροφοριακό σύστημα μισθοδοσίας και συντάξεων.

- C.4 *Tsohou A., Karyda M., Kokolakis S., Kiountouzis E., "Aligning Security Awareness with Information Systems Security Management", 4th Mediterranean Conference on Information*

Systems, September 2009, Athens, Greece

Τίτλος: «Ευθυγράμμιση της Ενημερότητας Ασφάλειας με τη Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων»

Στην παρούσα εργασία διερευνάται ο τρόπος με τον οποίο η διαδικασία της ενημερότητας ασφάλειας συνδέεται με το ευρύτερο πλαίσιο διοίκησης ασφάλειας πληροφοριακών συστημάτων (ΠΣ) το οποίο εξυπηρετεί. Μέχρι σήμερα, η διαμόρφωση πρωτοβουλιών ενημερότητας ασφάλειας αγνοεί την ιδιαίτερα σημαντική συσχέτιση με το συνολικό πλαίσιο διοίκησης ασφάλειας, και αντίστροφα. Σε αυτή την εργασία τεκμηριώνεται πώς οι δύο διεργασίες μπορούν να ευθυγραμμιστούν, ώστε να διασφαλίζεται ότι οι δραστηριότητες ενημερότητας εξυπηρετούν τη στρατηγική διοίκησης ασφάλειας, αλλά και ότι η διοίκηση ασφάλειας αξιοποιεί τα οφέλη από τις ενέργειες ενημερότητας. Αυτό πραγματοποιείται μέσα από την ανάλυση των δύο διεργασιών με χρήση ενός πλαισίου ανάλυσης οργανωσιακών διαδικασιών και στη συνέχεια με τη ανάλυση των αναδεικνυόμενων αλληλεπιδράσεων. Η αναγνώριση των αλληλεπιδράσεων αυτών έχει ως αποτέλεσμα να καθίσταται δυνατή η τοποθέτηση της ενημερότητας ασφάλειας στο ευρύτερο πλαίσιο διοίκησης ασφάλειας ΠΣ, σε αντίθεση με την αντιμετώπισή της ως έναν μεμονωμένο μηχανισμό ασφάλειας.

- C.3 *Tsohou A., Kokolakis S., Lambrinouidakis C., Gritzalis S., "Information Systems Security Management: A review and a classification of the ISO standards", In: Next Generation Society: Technological and Legal Issues, Springer Lecture Notes of the ICSSIT Institute for Computer Sciences, Social Informatics, and Telecommunications Engineering A. Sideridis and C. Patrikakis (Eds.), e-Democracy 2009, LNICST 26, pp. 220-235, 2010*

Τίτλος: «Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων: Επισκόπηση και Ταξινόμηση των ISO προτύπων»

Οι σχεδιαστές πληροφοριακών συστημάτων (ΠΣ) γνωρίζουν την αναγκαιότητα αμοιβαίας κατανόησης και συμφωνίας λειτουργικών και μη λειτουργικών προδιαγραφών ΠΣ. Η αναγκαιότητα αυτή αφορά τόσο το σχεδιασμό «ορθών» συστημάτων όσο και τη διαλειτουργικότητα με άλλα συστήματα. Ενδεικτικό παράδειγμα αυτής της αναγκαιότητας αποτελεί η ασφάλεια πληροφοριών. Στην περίπτωση που οι απαιτήσεις ασφάλειας δε γίνονται αντιληπτές με τον ίδιο τρόπο από όλα τα εμπλεκόμενα μέλη και οι μηχανισμοί ασφάλειας που θα υλοποιηθούν δεν ικανοποιούν διεθνώς αποδεκτούς κανόνες και πρακτικές, τότε το σύστημα που θα σχεδιαστεί είναι πιθανό να μην θα ικανοποιεί το επιθυμητό επίπεδο

ασφάλειας και θα είναι δύσκολο να διαλειτουργήσει ασφαλώς με άλλα ΠΣ. Είναι, λοιπόν, σαφής η συνεισφορά των διεθνών προτύπων για το σχεδιασμό και την υλοποίησης μηχανισμών ασφάλειας. Στην παρούσα εργασία παρουσιάζεται μία επισκόπηση των προτύπων διοίκησης ασφάλειας πληροφοριών που έχουν δημοσιευτεί από τον Διεθνή Οργανισμό Προτυποποίησης (International Organization for Standardization) και πραγματοποιείται ταξινόμησή τους σύμφωνα με τις έντεκα ενότητες μέτρων ασφάλειας του ISO/IEC 27001:2005. Η ανάλυση αυτή διευκολύνει τους επαγγελματίες ασφάλειας στην αποτελεσματική διοίκηση ασφάλειας πληροφοριών, καθώς η παρεχόμενη ταξινόμηση των προτύπων μπορεί να συνεισφέρει στην ενημέρωση και κατανόηση της πληθώρας προτύπων ασφάλειας που υπάρχουν.

- C.2 *Rizomiliotis P., Tsohou A., Lambrinouidakis C., Gritzalis S., "Security and Privacy Issues in Bipolar Disorder Research", ICICTH 7th International Conference on Information and Communication Technologies in Health, A. Hasman et al. (Eds.), July 2009, Samos, Greece, INEAG*

Τίτλος: «Ζητήματα Ασφάλειας και Ιδιωτικότητας στην Έρευνα Διπολικής Διαταραχής»

Παρά το γεγονός ότι υπάρχει ανάγκη έρευνας στο χώρο των ψυχικών ασθενειών, η σχετική έρευνα παρεμποδίζεται από τα ζητήματα εμπιστευτικότητας και προστασίας της ιδιωτικότητας που αφορούν τους ιατρικούς φακέλους. Η συγκέντρωση του ιατρικού ιστορικού ασθενών που πάσχουν από την ίδια ασθένεια σε κεντρικές βάσεις δεδομένων όπου μπορούν να εφαρμοστούν προηγμένες τεχνικές εξόρυξης γνώσης θα ήταν ιδιαίτερα πολύτιμες για τους ερευνητές. Η μεγαλύτερη πρόκληση είναι η ανωνυμοποίηση των δεδομένων, ώστε να ικανοποιούνται οι νομικές και ηθικές απαιτήσεις, ενώ παράλληλα να διατηρούνται οι κρίσιμες ιατρικές πληροφορίες. Στην παρούσα εργασία προτείνεται ένα μοντέλο δημιουργία κεντρικού αποθετηρίου ανωνυμοποιημένων δεδομένων ασθενών που πάσχουν από διπολική διαταραχή. Η γνώση αυτή τροφοδοτεί ένα ευφυές σύστημα που διευκολύνει και καθοδηγεί τους κλινικούς γιατρούς στη διαχείριση ασθενών. Οι απαιτήσεις ασφάλειας ικανοποιούνται από την εφαρμογή ελέγχου πρόσβασης με μηχανισμούς ελέγχου πρόσβασης βάσει ρόλων (Role Based Access Control).

- C.1 *Tsohou A., Theoharidou M., Kokolakis S., Gritzalis D.: "Addressing Cultural Dissimilarity in the Information Security Management Outsourcing Relationship", Proceedings of the TRUSTBUS'07, 4th International Conference on Trust, Privacy and Security in Digital*

Business, pp.24-33, Regensburg, Germany, September 2007, Lecture Notes in Computer Science LNCS, Springer.

Τίτλος: «Αντιμετωπίζοντας τα Ζητήματα Ανομοιότητας Κουλτούρας κατά την Εξωτερική Ανάθεση Διοίκησης Ασφάλειας Πληροφοριακών Συστημάτων»

Η οργανωσιακή κουλτούρα επηρεάζει τον τρόπο με τον οποίο α) γίνεται αντιληπτή η ασφάλεια πληροφοριών, β) εφαρμόζονται τα μέτρα ασφάλειας, και γ) αντιδρούν τα μέλη του οργανισμού στις αλλαγές κουλτούρας που απορρέουν από ένα νέο πρόγραμμα ασφάλειας. Στην περίπτωση εξωτερικής ανάθεσης της διοίκησης ασφάλειας πληροφοριακών συστημάτων είναι πιθανό να προκύψουν ζητήματα εξαιτίας της ανομοιότητας κουλτούρας ανάμεσα στον οργανισμό και τον εξωτερικό πάροχο, όπως για παράδειγμα σύγκρουση μεταξύ των μέτρων ασφάλειας που θέτει σε εφαρμογή ο πάροχος και τις εσωτερικές πολιτικές του οργανισμού. Στην παρούσα εργασία προτείνεται ένα εννοιολογικό πλαίσιο για την αναγνώριση και διαχείριση της ανομοιότητας κουλτούρας από τον οργανισμό στην περίπτωση εξωτερικής ανάθεσης της διοίκησης ασφάλειας πληροφοριακών συστημάτων.