ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

ΘΕΜΑΤΑ ΔΙΠΛΩΜΑΤΙΚΩΝ ΕΡΓΑΣΙΩΝ

(ΑΚΑΔΗΜΑΪΚΟ ΕΤΟΣ 2025-2026)

ΕΠΙΒΛΕΠΩΝ: ΧΡΗΣΤΟΣ ΞΕΝΑΚΗΣ

Α/Α	Θέμα Διπλωματικής Εργασίας	Σύντομη Περιγραφή [1]
1.	**Assurance Case Generator for Evidence-Driven Zero Trust Edge Services**	**Θεματική Περιοχή**: Trustworthy Systems, Security Assurance, Certification Evidence. Η εργασία θα αναπτύξει prototype tool για τη δημιουργία assurance cases σε Zero Trust edge services, όπου access decisions βασίζονται σε identity evidence, device posture, telemetry, audit logs και policy checks. **Μεθοδολογία**: ορισμός Claim-Argument-Evidence model, δημιουργία evidence schema, υλοποίηση assurance-case generator και εφαρμογή σε synthetic edge service authorization scenarios. **Αναμενόμενο αποτέλεσμα**: prototype generator, assurance-case templates, sample evidence sets και validation report που εντοπίζει missing evidence, weak claims και unsupported assumptions. **Εισηγητής-Ερευνητής:** Ιωάννης Στυλιανού
2.	**Compliance-as-Code Evidence Pack Generator for Kubernetes-based Cloud/Edge Services**	**Θεματική Περιοχή**: Continuous Certification, DevSecOps Evidence, Cloud Security. Θα σχεδιαστεί compliance-as-code framework που συλλέγει και

		οργανώνει machine-readable cybersecurity evidence για Kubernetes-based cloud/edge services. **Μεθοδολογία**: αξιοποίηση SBOMs, vulnerability scans, Kubernetes configuration checks, secrets detection, access-policy checks και API exposure analysis· mapping των αποτελεσμάτων σε control families και παραγωγή JSON/OSCAL-like evidence packs. **Αναμενόμενο αποτέλεσμα**: prototype evidence-pack generator, sample reports, gap analysis, remediation suggestions και αξιολόγηση σε 2-3 demo cloud/edge deployments. **Εισηγητής-Ερευνητής:** Ιωάννης Στυλιανού
3.	**Robustness Evaluation of AI-Driven Trustworthiness Decision Systems under Forecast Error and Telemetry Manipulation**	**Θεματική Περιοχή**: Adversarial AI, AI Assurance, Trustworthiness Decision Systems. Ανάπτυξη benchmark για AI-driven decision systems που εκτιμούν trust/risk και επιλέγουν security response levels βάσει telemetry, demand forecasts, anomaly indicators και policy constraints. **Μεθοδολογία**: δημιουργία synthetic dataset με normal, noisy και adversarial scenarios· εισαγωγή forecast errors, delayed telemetry, manipulated anomaly scores και missing evidence· αξιολόγηση rule-based, ML ή hybrid decision models. **Αναμενόμενο αποτέλεσμα**: benchmark dataset, attack scenarios, evaluation scripts και metrics όπως unsafe downgrade rate, false trust elevation, policy violation rate, fail-safe ratio και explanation consistency. **Εισηγητής-Ερευνητής:** Ιωάννης Στυλιανού Follow-up publication: "*Robustness Evaluation of AI-Driven Trustworthiness Decision Systems under Forecast Error and Telemetry Manipulation*"

4.	**Adaptive Zero Trust Policy Engine for API Access Control using Verifiable Trust Claims**	**Θεματική Περιοχή**: Zero Trust, Policy-as-Code, Verifiable Trust Claims. Υλοποίηση prototype policy engine για API access control, όπου οι αποφάσεις δεν βασίζονται μόνο σε roles αλλά σε dynamic trust claims όπως identity assurance, credential freshness, device posture, risk score, auditability και service sensitivity. **Μεθοδολογία**: ορισμός trust-claim schema, υλοποίηση policy model με Rego/OPA ή Python, synthetic API testbed και scenarios για revoked/expired claims, privilege escalation, conflicting claims, high-risk requests και step-up authentication. **Αναμενόμενο αποτέλεσμα**: policy engine, rule library, access-decision API και αξιολόγηση correctness, latency, explainability και robustness σε claim manipulation. **Εισηγητής-Ερευνητής:** Ιωάννης Στυλιανού
5.	**Privacy-Preserving Sharing of Vulnerability and Attestation Evidence between Security Domains**	**Θεματική Περιοχή**: Privacy-Preserving Security, Evidence Sharing, Federated Trust. Θα μελετήσει πώς δύο διαφορετικά security domains μπορούν να ανταλλάσσουν vulnerability και attestation evidence χωρίς αποκάλυψη raw logs, internal configurations, hostnames ή sensitive telemetry. **Μεθοδολογία**: δημιουργία synthetic evidence datasets, μοντελοποίηση raw evidence sharing, signed summaries, selective disclosure, hash commitments και privacy-preserving aggregates· συγκριτική αξιολόγηση ως προς audit usefulness, privacy leakage, evidence completeness και computational overhead. **Αναμενόμενο αποτέλεσμα**: prototype evidence-exchange mechanism, privacy-utility analysis και recommendations για cross-domain trust, auditability και certification evidence sharing. **Εισηγητής-Ερευνητής:** Ιωάννης Στυλιανού

6.	**Reinforcing Privacy through Federated Learning in Few Shot Transfer Learning Trust Prediction Systems in the IoT**	**Θεματική Περιοχή**: Few Shot Learning, Trust Prediction in IoT ecosystems, Federated Learning. **Μεθοδολογία**: ● Αρχικά θα γίνει μια ανασκόπηση στην βιβλιογραφία σχετικά με Federated Learning μεθόδους trust prediction για να προσδιοριστούν κενά στην παρούσες περιοχές και περιθώρια βελτίωσης. ● Ύστερα θα υλοποιηθεί ένα Federated Few-Shot Transfer Learning μοντέλο για πρόβλεψη trust score βασισμένου σε υπάρχον μοντέλο πρόβλεψης trust. Στο νέο μοντέλο η διαδικασία εκπαίδευσης θα πραγματοποιείται αποκεντρωμένα σε επίπεδο συσκευών και τα μοντέλα που εκπαιδεύονται σε κάθε συσκευή θα συνδυάζονται μέσω federated aggregation με στόχο την ενίσχυση ιδιωτικότητας χωρίς απώλεια ακρίβειας. **Αναμενόμενο αποτέλεσμα:** ● Ανάπτυξη και αξιολόγηση ενός privacy-preserving trust prediction συστήματος που επιτυγχάνει συγκρίσιμη ή βελτιωμένη απόδοση (MSE, MAE, R^2) σε σχέση με το centralized baseline, μειώνοντας παράλληλα τη διαρροή δεδομένων μέσω αποκεντρωμένης εκπαίδευσης, καθώς και παραγωγή πειραματικών αποτελεσμάτων και υλοποίησης. Η παρούσα διπλωματική θα βασιστεί στην δημοσίευση «Trust Score Prediction for IoT Device Onboarding Using Transfer and Few-Shot Learning in Consumer Electronics» **Εισηγητής ερευνητής:** Μιχαήλ Μπαμπάτσικος
7.	**Reinforcing the robustness of Explainable AI technologies against Adversarial AI attacks.**	**Θεματική Περιοχή:** Adversarial AI, Explainable AI, AI Security **Μεθοδολογία:**

		• Αρχικά θα πραγματοποιηθεί βιβλιογραφική ανασκόπηση σχετικά με τεχνικές XAI και τις ευπάθειες τους. Θα ακολουθήσει η ανάπτυξη ενός βασικού supervised learning μοντέλου για πρόβλεψη σε επιλεγμένο dataset (π.χ. classification σε security-related δεδομένα), το οποίο θα χρησιμοποιηθεί για την παραγωγή explanations. Θα ενσωματωθούν XAI μοντέλα (π.χ. SHAP και LIME) για την ερμηνεία των αποφάσεων του μοντέλου και καταγραφή των παραγόμενων explanations ως baseline. • Ύστερα θα πραγματοποιηθούν επιθέσεις που στοχεύουν στην δημιουργία παραπλανητικών explanations με μειωμένη σταθερότητα και συνέπεια. Επίσης θα πραγματοποιηθεί συγκριτική αξιολόγηση της απόδοσης των XAI μηχανισμών πριν και μετά την διεξαγωγή των επιθέσεων χρησιμοποιώντας μετρικές όπως: fidelity, stability, robustness και interpretability. **Αναμενόμενο αποτέλεσμα:** • Ένα πειραματικό framework αξιολόγησης XAI μοντέλων υπό adversarial AI επιθέσεις και ανάλυση της ευαισθησίας των μοντέλων αυτών. **Εισηγητής ερευνητής:** Μιχαήλ Μπαμπάτσικος
8.	**Detection and mitigation of adversarial poisoning attacks against few shot learning-based trust management frameworks.**	**Θεματική Περιοχή:** Adversarial AI, Few Shot Learning, Trust Management in IoT **Μεθοδολογία:** • Αρχικά θα πραγματοποιηθεί βιβλιογραφική ανασκόπηση σχετικά με adversarial poisoning attacks σε machine learning συστήματα και

		ειδικότερα σε few-shot learning μοντέλα. Στη συνέχεια θα υλοποιηθεί ένα baseline few-shot learning μοντέλο για classification ή prediction αξιοποιώντας ένα dataset με trust management related δεδομένα. Ύστερα θα σχεδιαστούν και θα εφαρμοστούν data poisoning attacks, όπου μέρος των training samples θα τροποποιείται με σκοπό την υποβάθμιση της απόδοσης του μοντέλου. Επίσης θα αναπτυχθεί μηχανισμός ανίχνευσης των poisoned samples βασισμένος σε στατιστικές αποκλίσεις. Στη συνέχεια θα υλοποιηθούν βασικές τεχνικές mitigation, όπως filtering των ύποπτων δειγμάτων ή robust training με καθαρά subsets δεδομένων, ή επανα-στάθμιση της επιρροής των training samples. Τέλος, θα πραγματοποιηθεί πειραματική αξιολόγηση της απόδοσης του συστήματος πριν και μετά τις επιθέσεις, καθώς και μετά την εφαρμογή των mitigation τεχνικών, με χρήση μετρικών όπως accuracy, F1-score, και attack success rate. **Αναμενόμενο αποτέλεσμα:** ● Ένα πειραματικό framework αξιολόγησης data poisoning attacks σε few-shot learning-based trust estimation συστήματα. ● Ανάπτυξη και αξιολόγηση μηχανισμού ανίχνευσης poisoned samples. ● Ανάλυση της ανθεκτικότητας few-shot μοντέλων σε adversarial επιθέσεις με συγκριτικά αποτελέσματα πριν και μετά την εφαρμογή mitigation τεχνικών. **Εισηγητής ερευνητής:** Μιχαήλ Μπαμπάτσικος

9.	**Μελέτη και ανάπτυξη πρωτοτύπου για υβριδικά ψηφιακά πιστοποιητικά X.509 με κλασικές και μετα-κβαντικές υπογραφές**	Η εργασία θα μελετήσει τη μετάβαση των υφιστάμενων υποδομών δημόσιου κλειδιού σε μετα-κβαντικό περιβάλλον, με έμφαση στη σχεδίαση υβριδικών πιστοποιητικών που συνδυάζουν κλασικούς αλγορίθμους, όπως ECDSA ή RSA, με post-quantum ψηφιακές υπογραφές. Η μεθοδολογία θα περιλαμβάνει βιβλιογραφική ανασκόπηση, ανάλυση σχετικών προτύπων, σχεδίαση δομής πιστοποιητικού και ανάπτυξη πρωτοτύπου έκδοσης και επαλήθευσης υβριδικών πιστοποιητικών. Το αναμενόμενο αποτέλεσμα είναι η **ανάπτυξη πρωτότυπου συστήματος και τεχνικής μελέτης** για υβριδικά X.509 πιστοποιητικά. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** Μετα-κβαντική Κρυπτογραφία, PKI, Ψηφιακά Πιστοποιητικά.

10.	**Σχεδίαση και υλοποίηση μηχανισμού Merkle-based πιστοποιητικών για quantum-resilient PKI**	Η εργασία θα εξετάσει τη χρήση Merkle trees ως μηχανισμού αυθεντικοποίησης και συμπίεσης αποδείξεων εγκυρότητας σε μετα-κβαντικές υποδομές πιστοποιητικών. Η μεθοδολογία θα περιλαμβάνει μαθηματική περιγραφή Merkle trees, σχεδίαση δομής Merkle-based certificate, ανάπτυξη εργαλείου δημιουργίας Merkle root και membership proofs, καθώς και πειραματική αξιολόγηση ως προς μέγεθος αποδείξεων, χρόνο επαλήθευσης και δυνατότητα ενσωμάτωσης σε PKI. Το τελικό παραδοτέο θα είναι η **ανάπτυξη πρωτότυπου Merkle Certificate Engine και συνοδευτική τεχνική αξιολόγηση**. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** QCERT, Merkle Trees, Post-Quantum PKI, Αυθεντικοποίηση.
11.	**Συγκριτική αξιολόγηση post-quantum αλγορίθμων υπογραφής για χρήση σε ψηφιακά πιστοποιητικά**	Η εργασία θα συγκρίνει μετα-κβαντικούς αλγορίθμους ψηφιακής υπογραφής ως προς την καταλληλότητά τους για χρήση σε PKI και ψηφιακά πιστοποιητικά (NIST standards αλλά και τα νέα submissions). Η μεθοδολογία θα περιλαμβάνει βιβλιογραφική και τεχνική ανάλυση αλγορίθμων, πειραματικές μετρήσεις χρόνου υπογραφής, χρόνου επαλήθευσης, μεγέθους δημόσιου κλειδιού, μεγέθους υπογραφής και επιπτώσεων στο μέγεθος πιστοποιητικών. Το αναμενόμενο αποτέλεσμα είναι η **εκπόνηση μελέτης και συγκριτικής αξιολόγησης** με σαφείς προτάσεις για την επιλογή αλγορίθμων στο πλαίσιο του QCERT. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** Post-Quantum Cryptography, Digital Signatures, PKI Evaluation.

12.	**Ανάπτυξη εργαλείου μετάβασης από κλασικά σε μετα-κβαντικά πιστοποιητικά σε υποδομές PKI**	Η εργασία θα σχεδιάσει και θα υλοποιήσει ένα εργαλείο που υποστηρίζει τη σταδιακή μετάβαση από κλασικά πιστοποιητικά σε υβριδικά ή πλήρως μετα-κβαντικά πιστοποιητικά. Η μεθοδολογία θα περιλαμβάνει ανάλυση υπάρχουσας PKI, ορισμό σεναρίων migration, σχεδίαση εργαλείου ελέγχου συμβατότητας και ανάπτυξη πρωτοτύπου που εντοπίζει πιστοποιητικά, αλγορίθμους και παραμέτρους που χρειάζονται αναβάθμιση. Το τελικό αποτέλεσμα θα είναι η **ανάπτυξη υπηρεσίας/εργαλείου migration readiness assessment** για οργανισμούς που προετοιμάζονται για post-quantum PKI. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** QCERT, PKI Migration, Cybersecurity Engineering.
13.	**Μελέτη και υλοποίηση PQC-aware TLS επικοινωνίας με χρήση μετα-κβαντικών μηχανισμών ανταλλαγής κλειδιού**	Η εργασία θα εξετάσει τον τρόπο ενσωμάτωσης μετα-κβαντικών μηχανισμών ανταλλαγής κλειδιού σε πρωτόκολλα ασφαλούς επικοινωνίας τύπου TLS. Η μεθοδολογία θα περιλαμβάνει μελέτη του TLS handshake, ανάλυση κλασικών και post-quantum key encapsulation mechanisms, υλοποίηση πειραματικού περιβάλλοντος client-server και αξιολόγηση επιδόσεων ως προς latency, μέγεθος μηνυμάτων και κόστος υπολογισμού. Το αναμενόμενο αποτέλεσμα είναι η **ανάπτυξη πειραματικού PQC-aware TLS prototype και τεχνική αξιολόγηση της λειτουργικότητάς του**. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** QCERT, TLS, Post-Quantum Key Exchange, Network Security.
14.	**Σχεδίαση Hybrid Certificate Authority Toolkit για έκδοση και διαχείριση post-quantum πιστοποιητικών**	Η εργασία θα εστιάσει στη σχεδίαση ενός εργαλείου αρχής πιστοποίησης που μπορεί να εκδίδει, να αποθηκεύει και να επαληθεύει υβριδικά ή μετα-κβαντικά πιστοποιητικά. Η μεθοδολογία θα περιλαμβάνει ανάλυση

		λειτουργιών μιας CA, σχεδίαση αρχιτεκτονικής, υλοποίηση βασικών λειτουργιών έκδοσης πιστοποιητικού, δημιουργίας αιτήματος πιστοποιητικού και επαλήθευσης αλυσίδας εμπιστοσύνης. Το τελικό παραδοτέο θα είναι η **ανάπτυξη πρωτότυπου Hybrid CA Toolkit**, συνοδευόμενου από τεχνική τεκμηρίωση και αξιολόγηση. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** QCERT, Certificate Authorities, Hybrid Cryptography, PKI.
15.	**Ανάλυση ασφαλείας και απειλών για μετα-κβαντικές υποδομές δημόσιου κλειδιού**	Η εργασία θα μελετήσει τις απειλές που αντιμετωπίζουν οι υποδομές δημόσιου κλειδιού στην εποχή των κβαντικών υπολογιστών, συμπεριλαμβανομένων επιθέσεων τύπου harvest-now-decrypt-later, προβλημάτων συμβατότητας και κινδύνων από λανθασμένη παραμετροποίηση. Η μεθοδολογία θα περιλαμβάνει threat modeling, ανάλυση σεναρίων επίθεσης, καταγραφή απαιτήσεων ασφαλείας και πρόταση αντιμέτρων για quantum-resilient PKI. Το αναμενόμενο αποτέλεσμα είναι η **εκπόνηση μελέτης ασφαλείας και προδιαγραφών προστασίας** για το οικοσύστημα QCERT. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** Cybersecurity, Threat Modeling, Post-Quantum PKI.
16.	**Εφαρμογή secret sharing για ασφαλή αποθήκευση ιδιωτικών κλειδιών σε post-quantum PKI**	Η εργασία θα διερευνήσει τη χρήση σχημάτων διαμοιρασμού μυστικού, όπως το Shamir Secret Sharing, για την προστασία ιδιωτικών κλειδιών σε αρχές πιστοποίησης και κρίσιμες PKI υποδομές. Η μεθοδολογία θα περιλαμβάνει μαθηματική ανάλυση του secret sharing, σχεδίαση πολιτικής threshold access, υλοποίηση εργαλείου διαμοιρασμού και ανακατασκευής κλειδιών και αξιολόγηση σε σενάρια διαχείρισης CA private keys. Το τελικό παραδοτέο θα είναι η **ανάπτυξη πρωτότυπου εργαλείου ασφαλούς διαχείρισης ιδιωτικών**

		κλειδιών με secret sharing. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** Secret Sharing, PKI Security, Key Management.
17.	**Threshold cryptography για κατανεμημένη έκδοση ψηφιακών πιστοποιητικών**	Η εργασία θα μελετήσει πώς τεχνικές threshold cryptography μπορούν να χρησιμοποιηθούν ώστε η έκδοση πιστοποιητικών να μη βασίζεται σε ένα μοναδικό ιδιωτικό κλειδί ή σε ένα μοναδικό σημείο αποτυχίας. Η μεθοδολογία θα περιλαμβάνει ανάλυση threshold signatures, σχεδίαση κατανεμημένου πρωτοκόλλου υπογραφής πιστοποιητικών, ανάπτυξη πρωτοτύπου με πολλαπλούς συμμετέχοντες και αξιολόγηση ως προς ασφάλεια, διαθεσιμότητα και κόστος επικοινωνίας. Το αναμενόμενο αποτέλεσμα είναι η **ανάπτυξη πειραματικού συστήματος threshold certificate signing**. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** Threshold Cryptography, Distributed PKI, Digital Signatures.
18.	**Υλοποίηση και αξιολόγηση Distributed Key Generation πρωτοκόλλου για κατανεμημένη διαχείριση κλειδιών**	Η εργασία θα εξετάσει πρωτόκολλα κατανεμημένης παραγωγής κλειδιών, όπως Feldman ή Pedersen DKG, με στόχο την ασφαλή δημιουργία κλειδιών χωρίς έμπιστο κεντρικό μέρος. Η μεθοδολογία θα περιλαμβάνει θεωρητική μελέτη των πρωτοκόλλων, υλοποίηση πειραματικού DKG συστήματος, προσομοίωση τίμιων και κακόβουλων συμμετεχόντων και αξιολόγηση ως προς επικοινωνιακό κόστος και ανθεκτικότητα. Το τελικό αποτέλεσμα θα είναι η **ανάπτυξη πρωτότυπου DKG συστήματος και πειραματική αξιολόγηση της ασφάλειας και απόδοσής του**. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** Distributed Key Generation, Secret Sharing, Threshold Cryptography.

19.	**Μελέτη εφαρμογής ομομορφικής κρυπτογράφησης για ασφαλή επεξεργασία δεδομένων κυβερνοασφάλειας**	Η εργασία θα εξετάσει πώς η ομομορφική κρυπτογράφηση μπορεί να επιτρέψει την επεξεργασία ευαίσθητων δεδομένων ασφαλείας χωρίς αποκρυπτογράφηση. Η μεθοδολογία θα περιλαμβάνει εισαγωγή σε partially, somewhat και fully homomorphic encryption, επιλογή κατάλληλου use case, όπως στατιστική ανάλυση logs ή encrypted risk scoring, υλοποίηση απλού πρωτοτύπου και μέτρηση κόστους υπολογισμού. Το τελικό αποτέλεσμα θα είναι η **εκπόνηση μελέτης και ανάπτυξη πειραματικού πρωτοτύπου ομομορφικής επεξεργασίας**. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** Homomorphic Encryption, Privacy-Preserving Computation, Cybersecurity.
20.	**Ανάπτυξη εκπαιδευτικής βιβλιοθήκης για Shamir Secret Sharing και εφαρμογές στην κρυπτογραφική διαχείριση κλειδιών**	Η εργασία θα έχει εκπαιδευτικό και ερευνητικό χαρακτήρα και θα στοχεύει στην ανάπτυξη βιβλιοθήκης που υλοποιεί το Shamir Secret Sharing με καθαρό, τεκμηριωμένο και επεκτάσιμο τρόπο. Η μεθοδολογία θα περιλαμβάνει μαθηματική θεμελίωση πεπερασμένων σωμάτων, υλοποίηση share generation και reconstruction, παραδείγματα χρήσης σε private key backup και πειραματική αξιολόγηση ορθότητας. Το τελικό παραδοτέο θα είναι η **ανάπτυξη εκπαιδευτικής κρυπτογραφικής βιβλιοθήκης και τεχνικής τεκμηρίωσης**. **Ερευνητής-Εισηγητής:** ΒΟΥΔΟΥΡΗΣ ΑΝΑΣΤΑΣΙΟΣ. **Θεματική Περιοχή:** Secret Sharing, Applied Cryptography, Key Management.
21.	**Μοντελοποίηση Γνώσης Κυβερνοασφάλειας για Χρηματοοικονομικά Περιβάλλοντα**	Η εργασία θα εστιάσει στον σχεδιασμό και την υλοποίηση ενός αρχικού μοντέλου γνώσης κυβερνοασφάλειας για χρηματοοικονομικά περιβάλλοντα. Το μοντέλο θα αποτυπώνει βασικές έννοιες και σχέσεις μεταξύ απειλών, ευπαθειών, περιουσιακών στοιχείων, δεικτών παραβίασης, τεχνικών επίθεσης, μέτρων προστασίας και κανονιστικών απαιτήσεων. Η εργασία

		μπορεί να αξιοποιήσει υφιστάμενα πρότυπα και μορφότυπα, όπως STIX/TAXII, MITRE ATT&CK, CAPEC, CWE/CVE και σχετικές απαιτήσεις συμμόρφωσης, ώστε να δημιουργηθεί μια συνεκτική αναπαράσταση γνώσης που θα μπορεί να χρησιμοποιηθεί από συστήματα ανάλυσης και λήψης αποφάσεων. **Τελικό αποτέλεσμα:** Ανάπτυξη συστήματος/υπηρεσίας σε μορφή prototype security knowledge graph, με τεκμηριωμένο data model, ενδεικτικό dataset, βασικά queries, μηχανισμό εισαγωγής/κανονικοποίησης CTI δεδομένων και τεχνική αναφορά που περιγράφει τον τρόπο αξιοποίησης του μοντέλου. **Θεματική Περιοχή:** Security Knowledge Modelling, Cyber Threat Intelligence, Ontologies, Knowledge Graphs. **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
22.	**Ανάλυση Γράφων για Ανίχνευση Ύποπτων Μοτίβων σε Συναλλακτικά Δεδομένα**	Η εργασία θα εστιάσει στην αναπαράσταση χρηματοοικονομικών συναλλαγών ως γράφου και στην ανάπτυξη τεχνικών ανάλυσης για τον εντοπισμό ύποπτων ή δυνητικά δόλιων συμπεριφορών. Οι κόμβοι του γράφου μπορούν να αναπαριστούν λογαριασμούς, χρήστες, συναλλαγές, συσκευές, εμπόρους, IP διευθύνσεις ή άλλα σχετικά στοιχεία, ενώ οι ακμές θα αποτυπώνουν σχέσεις και ροές συναλλαγών. Η εργασία θα διερευνήσει τεχνικές όπως pattern matching, centrality analysis, community detection, path analysis και anomaly scoring για την ανίχνευση μοτίβων όπως κυκλικές συναλλαγές, ταχεία μεταφορά κεφαλαίων, ύποπτες συστάδες λογαριασμών, structuring/smurfing και πιθανές coordinated fraud συμπεριφορές. **Τελικό αποτέλεσμα:** Ανάπτυξη συστήματος/υπηρεσίας σε μορφή prototype graph-based fraud detection engine, με graph schema, υλοποιημένους αλγορίθμους, Cypher queries ή αντίστοιχους graph queries, Python/NetworkX scripts, αξιολόγηση σε synthetic ή διαθέσιμο dataset και τεχνική τεκμηρίωση. **Θεματική Περιοχή:** Graph Analytics, Fraud Detection,

		Financial Cybersecurity, Anomaly Detection **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
23.	**Συσχέτιση Πληροφοριών Κυβερνοαπειλών και Γράφων Συναλλαγών για Εμπλουτισμένη Ανίχνευση Κινδύνων**	Η εργασία θα συνδυάσει τη μοντελοποίηση γνώσης κυβερνοασφάλειας με την ανάλυση γράφων συναλλαγών, με στόχο την παραγωγή πιο εμπλουτισμένων και context-aware ευρημάτων ασφάλειας. Η εργασία θα εξετάσει πώς πληροφορίες από CTI πηγές, όπως indicators of compromise, threat actors, attack techniques, malicious domains/IPs ή vulnerability references, μπορούν να συσχετιστούν με οντότητες ενός transaction graph, όπως λογαριασμούς, συσκευές, IP διευθύνσεις, χρήστες ή ύποπτα clusters συναλλαγών. Με αυτόν τον τρόπο, ένα ύποπτο χρηματοοικονομικό μοτίβο δεν θα αξιολογείται μόνο με βάση τη συμπεριφορά του γράφου, αλλά και με βάση το σχετικό threat context. **Τελικό αποτέλεσμα:** Ανάπτυξη συστήματος/υπηρεσίας σε μορφή prototype CTI-enriched graph analytics service, με μηχανισμό mapping μεταξύ CTI οντοτήτων και transaction graph entities, correlation logic, ενδεικτικό risk/context scoring, structured output για analysts ή LLM-based components, και συνοδευτική τεχνική μελέτη που εξηγεί το αποτέλεσμα. **Θεματική Περιοχή:** Cyber Threat Intelligence, Graph Analytics, Knowledge Graphs, Financial Threat Detection **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
24.	**Πρωτότυπο Διασύνδεσης Ψηφιακής Ταυτότητας με Αποκεντρωμένες Τεχνολογίες Ταυτοποίησης**	Η εργασία θα εστιάσει στη μελέτη και ανάπτυξη ενός απλού proof-of-concept εργαλείου/πλαισίου που διερευνά πώς μπορούν να συνδεθούν μηχανισμοί ψηφιακής ταυτότητας που ευθυγραμμίζονται με το eIDAS/eIDAS 2.0 με τεχνολογίες Self-Sovereign Identity (SSI). Ο στόχος είναι να σχεδιαστεί μια

		βασική γέφυρα διαλειτουργικότητας, όπου ένας χρήστης ή οργανισμός θα μπορεί να λαμβάνει, να αποθηκεύει και να παρουσιάζει επαληθεύσιμα διαπιστευτήρια μέσω SSI μηχανισμών, διατηρώντας παράλληλα συμβατότητα με ευρωπαϊκές απαιτήσεις εμπιστοσύνης, ταυτοποίησης και ψηφιακών πορτοφολιών. Η εργασία μπορεί να βασιστεί σε απλά σενάρια χρήσης για healthcare περιβάλλοντα, όπως επαλήθευση ρόλου επαγγελματία υγείας, ασφαλές onboarding χρήστη ή πρόσβαση σε ψηφιακή υπηρεσία υγείας. **Τελικό αποτέλεσμα:** Ανάπτυξη απλού prototype ή τεχνικού framework που δείχνει τη σύνδεση eIDAS/European Digital Identity Wallet λογικής με SSI/Verifiable Credentials, συνοδευόμενο από βασική αρχιτεκτονική, ροές χρήσης και τεχνική τεκμηρίωση. **Θεματική Περιοχή:** Digital Identity, eIDAS, Self-Sovereign Identity, Verifiable Credentials, Healthcare Cybersecurity. **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
25.	**Εκπαιδευτικό Πρωτότυπο Ευαισθητοποίησης στην Κυβερνοασφάλεια για Προσωπικό Υγείας (CyberGame-related)**	Η εργασία θα αφορά τον σχεδιασμό και την ανάπτυξη ενός μικρού web-based εκπαιδευτικού prototype για βασική ευαισθητοποίηση προσωπικού υγείας σε θέματα κυβερνοασφάλειας. Το περιεχόμενο μπορεί να περιλαμβάνει σύντομα μαθήματα, ερωτήσεις αξιολόγησης και απλά σενάρια, όπως phishing emails, ασφαλής χρήση κωδικών και βασικές πρακτικές προστασίας δεδομένων. **Τελικό αποτέλεσμα:** Ανάπτυξη απλής εκπαιδευτικής εφαρμογής ή mock-up με ενδεικτικό περιεχόμενο, quizzes και βασική παρακολούθηση προόδου χρήστη. **Θεματική Περιοχή:** Cybersecurity Awareness, Healthcare Training, Human-Centric Security, Phishing Awareness. **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
26.	**Εργαλείο Βασικής Αξιολόγησης Κυβερνοασφάλειας για Οργανισμούς Υγείας**	Η εργασία θα εστιάσει στη δημιουργία ενός απλού εργαλείου αξιολόγησης της κυβερνοασφάλειας για μικρούς ή μεσαίους οργανισμούς υγείας. Το

		εργαλείο θα βασίζεται σε ένα σύντομο ερωτηματολόγιο και θα καλύπτει βασικές περιοχές, όπως πρόσβαση χρηστών, ενημερώσεις συστημάτων, αντίγραφα ασφαλείας, εκπαίδευση προσωπικού και διαχείριση περιστατικών. **Τελικό αποτέλεσμα:** Ανάπτυξη απλού scoring tool που παράγει βασική βαθμολογία ωριμότητας, σύντομο gap analysis και ενδεικτικές προτάσεις βελτίωσης. **Θεματική Περιοχή:** Cyber Risk Assessment, Security Maturity, Healthcare Cybersecurity, Compliance Readiness. **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
27	**Ανάπτυξη Πρωτοτύπου Ελέγχου Συμμόρφωσης για AI-Based Cybersecurity Use Cases**	Η εργασία αφορά την ανάπτυξη ενός πρωτοτύπου εργαλείου για τον έλεγχο βασικών απαιτήσεων συμμόρφωσης σε AI-based cybersecurity use cases. Το εργαλείο θα χαρτογραφεί απαιτήσεις όπως logging, explainability, human oversight, data minimization και risk classification σε τεχνικούς ελέγχους και θα παρέχει ένδειξη συμμόρφωσης, εντοπισμό κενών και προτεινόμενες ενέργειες. **Τελικό αποτέλεσμα:** Ανάπτυξη Συστήματος / Υπηρεσίας, με λειτουργικό prototype και αξιολόγηση σε ενδεικτικό σενάριο IoT ή Critical Infrastructure. **Θεματική Περιοχή:** AI Governance, Cybersecurity Compliance, Cyber Risk Management, GDPR, EU AI Act. **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
28.	**Ανάπτυξη Πρωτοτύπου για Ημι-Αυτόματο Threat Modeling σε IoT Περιβάλλοντα**	Η εργασία αφορά την ανάπτυξη ενός πρωτοτύπου εργαλείου που υποστηρίζει το threat modeling και την αρχική αξιολόγηση κινδύνου σε IoT περιβάλλοντα. Το εργαλείο θα λαμβάνει ως είσοδο assets, συσκευές, συνδέσεις, ευπάθειες και controls, και θα παράγει πιθανές απειλές, attack paths και βασική βαθμολόγηση κινδύνου. **Τελικό αποτέλεσμα:** Ανάπτυξη Συστήματος / Υπηρεσίας, βασισμένη σε graph-based αναπαράσταση και αξιολόγηση σε synthetic IoT use case. **Θεματική Περιοχή:** Threat Modeling,

		IoT Security, Cyber Risk Scoring, Knowledge Graphs, Critical Infrastructure Protection. **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
29.	**Ανάπτυξη Μηχανισμού Εξηγήσιμων Alerts για AI-Based Threat Detection**	Η εργασία αφορά την ανάπτυξη ενός XAI module για την ερμηνεία alerts που παράγονται από AI-based threat detection ή anomaly detection μοντέλα. Το module θα χρησιμοποιεί τεχνικές όπως SHAP ή LIME για να εξηγεί ποια χαρακτηριστικά επηρέασαν την απόφαση του μοντέλου και να παράγει κατανοητές εξηγήσεις για security analysts. **Τελικό αποτέλεσμα:** Ανάπτυξη Συστήματος / Υπηρεσίας, με λειτουργικό prototype και πειραματική αξιολόγηση σε cybersecurity dataset ή synthetic scenario. **Θεματική Περιοχή:** Explainable AI, Threat Detection, Incident Response, Human-in-the-Loop Cybersecurity, Cyber Risk Management. **Ερευνητής-Εισηγητής**: Ιωάννης Χουχουλής
30.	**Cyber Hygiene Assessment Framework για οργανισμούς υγείας**	**Θεματική Περιοχή**: Cyber Hygiene / Security Awareness / Healthcare Security **Περιγραφή**: Η εργασία αφορά τη σχεδίαση και αξιολόγηση ενός framework μέτρησης cyber hygiene για οργανισμούς υγείας, με έμφαση σε καθημερινές πρακτικές χρηστών και διαχειριστών συστημάτων. Το framework θα βασίζεται σε διεθνή πρότυπα (NIST CSF, CIS Controls, ENISA good practices) και θα προσαρμόζεται στις ιδιαιτερότητες του healthcare environment. **Μεθοδολογία**: ● Βιβλιογραφική ανασκόπηση σε cyber hygiene metrics. ● Καταγραφή κρίσιμων πρακτικών cyber hygiene. ● Δημιουργία ερωτηματολογίου ή scoring model.

		• Πιλοτική εφαρμογή σε εργαστηριακό ή πραγματικό περιβάλλον. • Στατιστική ανάλυση αποτελεσμάτων και εξαγωγή δεικτών ωριμότητας. **Αναμενόμενο Αποτέλεσμα**: • Cyber hygiene assessment model. • Ενσωμάτωση σε ISMS. • Πίνακας maturity scoring. • Dashboard ή proof-of-concept reporting tool. • Προτάσεις βελτίωσης για healthcare οργανισμούς. **Ερευνητής-Εισηγητής:** Απόστολος Κουτσουλέλος
31.	**Ανάλυση της Αποτελεσματικότητας Security Awareness Campaigns μέσω Προσομοιώσεων και Παιγνίων**	**Θεματική Περιοχή**: Human Factor Security / Awareness / Social Engineering **Περιγραφή**: Η εργασία εξετάζει κατά πόσο οι εκπαιδευτικές δράσεις awareness μέσω προσομοιώσεων και παιγνίων αυξάνουν το επίπεδο ευαισθητοποίησης. Ο φοιτητής θα χρησιμοποιήσει προσομοιώσεις και παίγνια και θα αξιολογήσει τη συμπεριφορά χρηστών πριν και μετά από awareness interventions. **Μεθοδολογία**: • Μελέτη phishing tactics και human-centered attacks. • Σχεδιασμός simulated phishing campaigns. • Συλλογή metrics (click rate, credential submission, reporting rate). • Σχεδίαση awareness material. • Επαναληπτική μέτρηση και comparative analysis. **Αναμενόμενο Αποτέλεσμα**:

		• Μετρήσιμο framework αξιολόγησης awareness effectiveness. • Comparative study πριν/μετά την εκπαίδευση. • Recommendations για awareness optimization. • Dataset και στατιστική ανάλυση αποτελεσμάτων. **Ερευνητής-Εισηγητής:** Απόστολος Κουτσουλέλος
32.	**Αξιολόγηση της Ασφάλειας και Συμμόρφωσης AI-based Applications σε Εταιρικά Περιβάλλοντα**	**Θεματική Περιοχή**: AI Security / AI Governance / AI Act / Compliance **Περιγραφή**: Η εργασία εξετάζει κινδύνους ασφαλείας και συμμόρφωσης από τη χρήση generative AI εφαρμογών σε οργανισμούς. Εστιάζει σε data leakage, prompt injection, shadow AI usage και governance controls. **Μεθοδολογία**: • Καταγραφή AI-related threat landscape. • Μελέτη OWASP Top 10 for LLM Applications. • Δημιουργία risk assessment framework. • Τεχνικές δοκιμές prompt injection ή data exposure. • Mapping με ISO 27001, NIS2 και AI Act requirements. **Αναμενόμενο Αποτέλεσμα**: • AI security assessment methodology. • Checklist ασφαλούς υιοθέτησης AI εργαλείων. • Proof-of-concept testing scenarios. • Προτάσεις governance και technical controls. **Ερευνητής-Εισηγητής:** Απόστολος Κουτσουλέλος

33.	**Αξιολόγηση της Ωριμότητας ISMS σε Μεσαίους Οργανισμούς βάσει ISO 27001 και NIS2**	**Θεματική Περιοχή**: ISMS / Governance / Compliance Engineering **Περιγραφή**: Η εργασία εξετάζει την πρακτική εφαρμογή ISMS frameworks σε οργανισμούς μεσαίου μεγέθους και αναλύει τα τεχνικά και οργανωτικά κενά σε σχέση με ISO 27001 και NIS2. **Μεθοδολογία**: ● Μελέτη ISO 27001 controls και NIS2 requirements. ● Δημιουργία maturity assessment matrix. ● Gap analysis σε επιλεγμένο οργανισμό ή case study. ● Καταγραφή technical και procedural deficiencies. ● Prioritization remediation plan. **Αναμενόμενο Αποτέλεσμα**: ● ISMS maturity model. ● Gap analysis report. ● Risk prioritization framework. ● Roadmap συμμόρφωσης και βελτίωσης. **Ερευνητής-Εισηγητής:** Απόστολος Κουτσουλέλος
34.	**Μεθοδολογία Σύνταξης Ψηφιακής Πραγματογνωμοσύνης για Δικαστική Χρήση**	**Θεματική Περιοχή**: Digital Forensics / Incident Investigation / Cybercrime Investigation **Περιγραφή**: Η εργασία αφορά τη μελέτη και εφαρμογή μεθοδολογιών σύνταξης ψηφιακών πραγματογνωμοσυνών (digital forensic reports) με στόχο τη χρήση τους σε δικαστικές ή πειθαρχικές διαδικασίες. Ιδιαίτερη έμφαση δίνεται στη σωστή τεκμηρίωση ευρημάτων, στη διατήρηση chain of

		custody και στη μετατροπή τεχνικών δεδομένων σε κατανοητό και αποδεικτικά αξιοποιήσιμο υλικό. **Μεθοδολογία**: ● Μελέτη διεθνών forensic standards και guidelines (NIST, ACPO, ENFSI). ● Ανάλυση δομής πραγματικών forensic reports. ● Δημιουργία controlled forensic scenario (π.χ. phishing incident, insider activity, malware infection). ● Συλλογή και ανάλυση ψηφιακών πειστηρίων. ● Τεκμηρίωση chain of custody. ● Σύνταξη πλήρους forensic report με τεχνικά παραρτήματα και executive summary. **Αναμενόμενο Αποτέλεσμα**: ● Πλήρης ψηφιακή πραγματογνωμοσύνη βασισμένη σε πραγματικό ή εργαστηριακό περιστατικό. ● Πρότυπο (template) forensic reporting. ● Οδηγός βέλτιστων πρακτικών για παρουσίαση ψηφιακών αποδείξεων. ● Τεκμηριωμένη διαδικασία preservation και admissibility evidence. **Ερευνητής-Εισηγητής:** Απόστολος Κουτσουλέλος
35.	**Ανάλυση και Τεκμηρίωση Ψηφιακών Πειστηρίων από Desktop**	**Θεματική Περιοχή**: Digital Forensics / Cloud Forensics / Endpoint Investigation

	(Windows/Linux/MacOS) και Cloud Περιβάλλοντα	**Περιγραφή**: Η εργασία εξετάζει τη διαδικασία συλλογής, ανάλυσης και τεκμηρίωσης ψηφιακών πειστηρίων από σύγχρονα endpoint και cloud περιβάλλοντα. Στόχος είναι η ανάπτυξη μεθοδολογίας παραγωγής τεχνικών αναφορών που μπορούν να αξιοποιηθούν σε incident response, εσωτερικούς ελέγχους ή δικαστικές/πειθαρχικές διαδικασίες. **Μεθοδολογία**: ● Μελέτη artifact analysis σε desktop systems και cloud services. ● Συλλογή forensic artifacts (logs, browser artifacts, event logs, cloud activity logs). ● Χρήση εργαλείων όπως Autopsy, FTK Imager, Velociraptor ή KAPE. ● Reconstruction timeline συμβάντων. ● Τεκμηρίωση ευρημάτων και αξιολόγηση αξιοπιστίας δεδομένων. ● Σύνταξη τεχνικής και μη τεχνικής αναφοράς. **Αναμενόμενο Αποτέλεσμα**: ● Forensic investigation report πλήρως τεκμηριωμένο. ● Timeline analysis συμβάντος ασφαλείας. ● Καταγραφή διαδικασίας συλλογής και preservation evidence. ● Οδηγός reporting για cloud και endpoint investigations. **Ερευνητής-Εισηγητής:** Απόστολος Κουτσουλέλος
36.	**Adversarial Robustness of LLM-Based Cybersecurity Agents – Automated Red-Teaming and Prompt-Injection Mitigation**	**Objectives** 1. Build an automated red-teaming pipeline for LLM agents performing cyber tasks (log analysis, incident response, code patching). 2. Design and evaluate hybrid defenses (guardrails + adversarial fine-tuning + output filtering).

		3. Create the first public benchmark dataset of adversarial prompts for cybersecurity agents **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
37.	**Adversarial Robustness Evaluation, Detection, and Mitigation for Small Language Model**	**Objectives** 1. Conduct a systematic robustness evaluation of state-of-the-art SLMs in realistic cybersecurity tasks (e.g., cyber threat classification, log analysis, incident response agents). 2. Develop and benchmark automated detection methods for adversarial prompts (prompt injection/jailbreaks) optimized for SLM inference constraints. 3. Design and evaluate practical mitigation strategies (hybrid guardrails + selective adversarial fine-tuning) that preserve utility while reducing attack success rate (ASR). 4. Release an open-source evaluation harness + cyber-specific adversarial benchmark dataset. **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
38.	**Development of an AI-Enhanced Open-Source SOC Framework with Adversarial Robustness and Economic Evaluation**	**Objectives** 1. Design and deploy a fully functional, modular open-source SOC stack using state-of-the-art 2026 tools. 2. Integrate SLM-based AI modules for automated threat classification, incident summarization, and play-book generation. 3. Conduct systematic adversarial robustness evaluation (prompt injection/jailbreak attacks on SLM components + evasion on traditional ML detectors).

		4. Develop detection and mitigation strategies tailored to SOC constraints (low latency, edge compatibility). 5. Perform a cybersecurity economics analysis (total cost of ownership, ROI, attack surface reduction) compared to commercial alternatives. **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
39.	**Adversarial AI for Poisoning Medical Data Analysis**	**Objectives** 1. Perform the evaluation of the adversarial AI (FGSM, BIM, PGD and CW) to generate adversarial examples for medical image analysis to avoid simultaneously multiple diagnostic AI models (diagnosis multi-evasion). 2. Evaluation metrics will be the attack success rate (ASR) as well as the computational efficiency of the proposed attacks in terms of i) latency (i.e., time taken by the method to generate the attack sample) and ii) Sparsity (the changes made to the features by the method to generate the adversarial image). 3. White box, black box and grey box scenarios will be considered as well as dataset and model poisoning scenarios will be examined and numerical results will be reported. **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
40.	**Adversarial AI for Bypassing Medical IoT Malware Detection**	**Objectives** 1. Generate adversarial examples capable of bypassing several defensive methods of AI-powered virus detection methods

		2. Investigate and uniquely combine different techniques, such as gradient-based techniques (Projected Gradient Descent, DeepFool, Fast Gradient Sign) for adversarial AI tests. 3. Transferability of diagnosis evasion will be evaluated for malware evasion. 4. Poisoning attacks (mainly backdoor) and evasion will be considered for testing purposes. Malware evasion rates and detection rates will be reported for various malware families with different purposes (data exfiltration, ransomware) **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
41.	**Adversarial AI for Evading Medical IoT Intrusion Detection**	**Objectives** 1. Generate adversarial traffic to evade an IDS. 2. Using a GAN model with variational autoencoder for learning a smooth and structured representation of the network traffic flow. This will expedite the generation of effective adversarial samples. 3. Poisoning the dataset will be considered but more importantly backdoor attacks will be investigated by identifying fields within IoT protocol packets that can be backdoored and strongly influence the IDS classifier predictions. 4. Adversarial attack success will be reported as well as performance degradation in case of backdoored packet presence. 5. Moreover, will also ensure that the generated traffic is still realistic and does violate any medical IoT protocol rule. **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ

42.	**Robust AI for Trustworthy Medical Data Analysis**	**Objectives** 1. Develop robust AI diagnosis for medical images. 2. Research and development will focus on a novel combination of image-level pre-processing, robust learning, and detection through explainability to identify adversarialsamples without compromising the performance of medical image analysis. 3. Various explainability methods will be utilized including methods like RuleFit, LIME, and SHAP, for interpretable results that will allow the development of robust diagnostic AI models. 4. Accuracy results of the robust AI model will be reported under adversarial and non-adversarial scenarios to explore whether robustness comes with a tradeoff in the clean performance of the AI diagnostic model. **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
43.	**Robust AI for Trustworthy Medical IoT Malware Detection**	**Objectives:** 1. Focus on a robust learning method to detect medical IoT malware by integrating training with adversarial samples and testing with perturbation control. 2. Evaluate and derive new robustness evaluation parameters and for this reason will adapt, enhance and utilize the AdvCat framework (also other frameworks will be considered such as URET) to evaluate the adversarial robustness of medical IoT malware classifiers. 3. The classifier will be evaluated using adversarial and non-adversarial samples. 4. Various malware families will be considered for fair assessment **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ

44.	**Robust AI for Trustworthy Medical IoT Intrusion Detection**	**Objectives** 1. Develop an attack-agnostic robust IDS using adversarial training and perturbation control enhanced with explainable AI framework. 2. Explainability for the IDS engine will include also visualization as blue teams and defenders prefer to visually inspect the network traffic and comprehend the alerts. 3. The explainable AI will fortify the confidence of the results as it will quickly allow the interpretation of the decision making. 4. Will evaluate the robustness of the AI model for the IDS under adversarial and non-adversarial network traffic. **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
45.	**AI-Integrated Dynamic Cybersecurity Risk Assessment Framework with Explainability and Economic Quantification**	**Objectives** 1. Design and implement a modular AI-powered risk assessment framework aligned with NIST CSF 2.0 + AI RMF. 2. Develop automated pipelines for dynamic risk scoring using multi-modal inputs (assets, vulnerabilities, threat intel, logs). 3. Integrate explainable AI techniques (SHAP, LIME, attention visualization) for transparent risk decisions. 4. Incorporate cybersecurity economics modeling to translate technical risks into monetary impact and mitigation ROI. 5. Evaluate the framework in realistic lab scenarios and release it as fully open-source with a benchmark dataset. **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
46.	**Open-Source AI Cybersecurity Risk Assessment Framework for AI Systems – Practical Implementation of the NIST Cyber AI Profile**	**Objectives**

	(NISTIR 8596) with Adversarial Robustness Testing and Economic Quantification	1. Design and implement a modular open-source risk assessment platform fully aligned with the NIST Cyber AI Profile (Secure AI components, AI-enabled defense, and governance functions). 2. Develop automated pipelines for ingesting AI system descriptions/models and producing risk profiles (including AIVSS scoring). 3. Integrate adversarial evaluation (prompt injection, data poisoning, model extraction attacks) tailored to AI systems used in cybersecurity contexts. 4. Add quantitative economic modeling to translate technical risks into monetary impact and prioritized mitigation ROI. 5. Release the complete framework, evaluation harness, and a new benchmark dataset as open-source artifacts **Ερευνητής-Εισηγητής:** Αριστείδης Φαραώ
47.	**Explainability Consistency Evaluation under Adversarial Perturbations in Cybersecurity AI Systems**	**Θεματική Περιοχή:** Explainable AI, Adversarial AI, AI Security **Μεθοδολογία:** Η εργασία θα μελετήσει πώς adversarial perturbations επηρεάζουν τη σταθερότητα και αξιοπιστία explainability μηχανισμών σε AI-based cybersecurity systems. Θα αναπτυχθούν baseline classification models για cybersecurity datasets και θα ενσωματωθούν explainability τεχνικές όπως SHAP, LIME και Integrated Gradients. Στη συνέχεια θα εφαρμοστούν adversarial attacks και θα αξιολογηθεί η μεταβολή explanations μέσω metrics όπως explanation drift, fidelity, stability και consistency. **Αναμενόμενο Αποτέλεσμα:**

		1. Experimental framework αξιολόγησης XAI robustness. 2. Comparative analysis explainability degradation. 3. Visualization toolkit για explanation instability. 4. Benchmark results για adversarially perturbed explanations. **Ερευνητής-Εισηγητής:** Στυλιανός Μπατζάκας
48.	**AI-Generated Synthetic Network Traffic for Cybersecurity Dataset Augmentation**	**Θεματική Περιοχή:** Synthetic Data Generation, Cybersecurity AI, Network Security **Μεθοδολογία:** Η εργασία θα αναπτύξει pipeline δημιουργίας synthetic network traffic μέσω generative AI τεχνικών για ενίσχυση cybersecurity datasets. Θα μελετηθούν GANs, diffusion models και sequence generation architectures για παραγωγή realistic traffic flows και attack scenarios. Θα αξιολογηθεί η ποιότητα των synthetic δεδομένων μέσω statistical similarity, protocol validity και downstream IDS performance. **Αναμενόμενο Αποτέλεσμα:** 1. Synthetic traffic generation framework. 2. Comparative evaluation διαφορετικών generative approaches. 3. Dataset augmentation pipeline για IDS training. 4. Experimental evaluation realism και utility. **Ερευνητής-Εισηγητής:** Στυλιανός Μπατζάκας

49.	**Benchmarking Prompt Injection Attacks against Small Language Models in Cybersecurity Tasks**	**Θεματική Περιοχή:** LLM Security, Adversarial AI, Cybersecurity Agents **Μεθοδολογία:** Η εργασία θα μελετήσει prompt injection και jailbreak επιθέσεις σε Small Language Models που χρησιμοποιούνται σε cybersecurity tasks. Θα δημιουργηθεί benchmark με adversarial prompts για log analysis, alert summarization και threat classification. Θα αξιολογηθούν διαφορετικές defense strategies όπως output filtering, prompt hardening και contextual isolation. **Αναμενόμενο Αποτέλεσμα:** 1. Open benchmark adversarial prompts. 2. Evaluation harness για SLM robustness testing. 3. Comparative analysis attack success rates. 4. Recommendations για ασφαλή χρήση SLMs. **Ερευνητής-Εισηγητής:** Στυλιανός Μπατζάκας
50.	**Graph-Based Threat Correlation for Multi-Stage Cyber Attack Analysis**	**Θεματική Περιοχή:** Graph Analytics, Cyber Threat Intelligence, Attack Correlation **Μεθοδολογία:** Η εργασία θα εστιάσει στην αναπαράσταση cyber attacks ως attack graphs και στη συσχέτιση multi-stage attack events. Θα αξιοποιηθούν graph-based techniques, MITRE ATT&CK mappings και anomaly propagation algorithms για correlation διαφορετικών security alerts και indicators. Θα αναπτυχθεί prototype visualization και risk scoring pipeline.

		Αναμενόμενο Αποτέλεσμα: 1. Prototype graph-based threat correlation engine. 2. Multi-stage attack visualization framework. 3. Experimental attack path analysis. 4. Risk prioritization scoring system. **Ερευνητής-Εισηγητής:** Στυλιανός Μπατζάκας
51.	**Explainable Risk Scoring for AI-Based Cybersecurity Monitoring Systems**	**Θεματική Περιοχή:** Explainable AI, Risk Scoring, SOC Analytics **Μεθοδολογία:** Η εργασία θα αναπτύξει explainable AI risk scoring framework για cybersecurity monitoring systems και SOC environments. Θα συλλέγονται alerts, anomalies και telemetry δεδομένα και θα δημιουργείται δυναμικό risk scoring με explainability support μέσω SHAP/LIME και attention visualization techniques. Θα αξιολογηθεί interpretability, alert prioritization quality και analyst usability. **Αναμενόμενο Αποτέλεσμα:** 1. Explainable cybersecurity risk scoring framework. 2. Prototype SOC-oriented dashboard. 3. Comparative evaluation explainability techniques. 4. Analyst-centric alert prioritization evaluation. **Ερευνητής-Εισηγητής:** Στυλιανός Μπατζάκας

52.	**Detection of Coordinated Cyber Attacks using Temporal Graph Neural Networks**	**Θεματική Περιοχή:** Graph Neural Networks, Cyber Threat Detection, Temporal Analytics **Μεθοδολογία:** Η εργασία θα εξετάσει τη χρήση Temporal Graph Neural Networks για ανίχνευση coordinated cyber attacks. Network entities και security events θα αναπαρίστανται ως evolving graph structures. Θα αξιολογηθούν temporal embeddings, anomaly propagation και attack pattern recognition techniques σε multi-stage attack scenarios. **Αναμενόμενο Αποτέλεσμα:** 1. Temporal cyber attack graph framework. 2. Comparative evaluation GNN architectures. 3. Coordinated attack detection pipeline. 4. Experimental results σε evolving attack scenarios. **Ερευνητής-Εισηγητής:** Στυλιανός Μπατζάκας
53.	**Taxonomy on Educational Material Regarding Cybersecurity**	**Θεματική Περιοχή** Cybersecurity Education, Knowledge Representation, Ontologies, Learning Analytics **Μεθοδολογία** Αρχικά θα πραγματοποιηθεί εκτενής βιβλιογραφική ανασκόπηση σε προσεγγίσεις ταξινόμησης εκπαιδευτικού περιεχομένου στον τομέα της

		κυβερνοασφάλειας, καθώς και σε συναφή πεδία όπως learning taxonomies (Bloom-based models), ontologies για knowledge representation και semantic educational data modeling. Στη συνέχεια θα συλλεχθεί και θα αναλυθεί ετερογενές εκπαιδευτικό υλικό κυβερνοασφάλειας, το οποίο μπορεί να περιλαμβάνει πανεπιστημιακές σημειώσεις, εκπαιδευτικά εργαστήρια (labs), υλικό πιστοποιήσεων (π.χ. ISO/NIST-aligned training), καθώς και ανοικτά online courses. Με βάση την ανάλυση αυτή θα σχεδιαστεί μια πολυεπίπεδη taxonomic δομή, η οποία θα περιλαμβάνει: ● θεματικές περιοχές κυβερνοασφάλειας (π.χ. network security, application security, AI security) ● επίπεδα γνώσης (introductory, intermediate, advanced) ● τύπους δεξιοτήτων (theoretical, analytical, hands-on) ● mapping σε learning outcomes Παράλληλα, θα διερευνηθεί η χρήση NLP τεχνικών και embedding-based clustering για την αυτόματη αντιστοίχιση εκπαιδευτικού υλικού σε nodes της taxonomy. Τέλος, θα πραγματοποιηθεί αξιολόγηση της προτεινόμενης ταξινομίας μέσω expert validation (instructors / cybersecurity practitioners) και μέσω metrics κάλυψης, συνέπειας και επεκτασιμότητας.

		Αναμενόμενο Αποτέλεσμα Η διπλωματική θα οδηγήσει στην ανάπτυξη ενός ολοκληρωμένου Cybersecurity Education Taxonomy Framework, το οποίο θα μπορεί να χρησιμοποιηθεί ως βάση για την οργάνωση και ανάλυση εκπαιδευτικού περιεχομένου. Παράλληλα θα υλοποιηθεί: ● Interactive web-based taxonomy explorer, όπου ο χρήστης θα μπορεί να πλοηγείται σε concepts και εκπαιδευτικό υλικό ● Annotated dataset εκπαιδευτικού υλικού mapped στην προτεινόμενη taxonomy ● Semantic search μηχανισμός για retrieval εκπαιδευτικών πόρων Το τελικό σύστημα θα μπορεί να υποστηρίξει use cases όπως curriculum design, adaptive learning και skill-gap analysis. **Ερευνήτρια-Εισηγήτρια:** Κατερίνα Ψυχογυιού
54.	**AI Model for Visualisation & Gamification of Scenarios**	**Θεματική Περιοχή** Generative AI, Educational Technology, Simulation Systems, Cybersecurity Training **Μεθοδολογία**

		Αρχικά θα πραγματοποιηθεί ανασκόπηση της βιβλιογραφίας σε τομείς generative AI for multimodal content creation, εκπαιδευτική προσομοίωση και gamification τεχνικών για cybersecurity training environments. Στη συνέχεια θα σχεδιαστεί και θα υλοποιηθεί ένα AI-based multimodal generation system, το οποίο θα μετατρέπει structured scenario scripts (π.χ. incident descriptions, attack flows, training narratives) σε οπτικοποιημένο εκπαιδευτικό περιεχόμενο. Το σύστημα θα περιλαμβάνει: ● NLP pipeline για parsing script-based scenarios ● scenario-to-event decomposition engine (timeline extraction) ● generative module για εικόνες (diffusion models ή APIs) και animation sequences ● GIF/video synthesis layer για δημιουργία δυναμικών visual scenarios Επιπλέον θα διερευνηθεί η ενσωμάτωση gamification logic, όπου κάθε scenario μπορεί να μετατραπεί σε interactive learning experience με: ● decision points ● branching outcomes ● scoring / feedback mechanisms Για την αξιολόγηση θα χρησιμοποιηθούν metrics όπως:

		• semantic fidelity (αντιστοίχιση script → visual output) • user engagement σε εκπαιδευτικά tests • correctness of scenario representation **Ερευνήτρια-Εισηγήτρια:** Κατερίνα Ψυχογυιού
55.	**Design & Development of a vulnerability assessment tool for AI systems.**	ENG: This thesis will focus on the design and development of a web-based application for the assessment of vulnerabilities of AI systems. Specifically, the application should be able to process AIBOM (AI Bill Of Material) files (generated via the OWASP AIBOM Open-source generator https://genai.owasp.org/resource/owasp-aibom-generator/) and search in public vulnerability repositories (e.g., NVD https://nvd.nist.gov/) for vulnerabilities in the packages that constitute the AIBOM. The application should have a user-friendly interface for uploading the AIBOM and presenting the different files (contents of the AIBOM in a list), as well as present the results of the discovered vulnerabilities including their severity and CVSS score. Areas: AI Security, AI Bill Of Materials, Vulnerabilities of AI systems Expected Result: Web-based application for uploading and presenting the contents of an AIBOM and the analysis, detection of vulnerabilities and presentation of vulnerabilities including through the NVD database. GR: Αυτή η διπλωματική εργασία θα επικεντρωθεί στον σχεδιασμό και την ανάπτυξη μιας διαδικτυακής εφαρμογής για την αξιολόγηση ευπαθειών συστημάτων AI. Συγκεκριμένα, η εφαρμογή θα πρέπει να είναι σε θέση να

		επεξεργάζεται αρχεία AIBOM (τα οποία δημιουργούνται μέσω του OWASP AIBOM Open-source generator https://genai.owasp.org/resource/owasp-aibom-generator/) και να πραγματοποιεί αναζήτηση σε δημόσια αποθετήρια ευπαθειών (π.χ. NVD https://nvd.nist.gov/) για ευπάθειες στα πακέτα που αποτελούν το AIBOM. Η εφαρμογή θα πρέπει να διαθέτει φιλικό προς τον χρήστη περιβάλλον για τη μεταφόρτωση του AIBOM και την παρουσίαση των διαφορετικών αρχείων (των περιεχομένων του AIBOM σε μορφή λίστας), καθώς και να παρουσιάζει τα αποτελέσματα των εντοπισμένων ευπαθειών, συμπεριλαμβανομένου του Severity και της βαθμολογίας CVSS. Τομείς: AI Security, AI Bill Of Materials, Ευπάθειες συστημάτων AI Αναμενόμενο Αποτέλεσμα: Διαδικτυακή εφαρμογή για τη μεταφόρτωση και παρουσίαση των περιεχομένων ενός AIBOM, καθώς και για την ανάλυση, τον εντοπισμό και την παρουσίαση ευπαθειών, συμπεριλαμβανομένης της αξιοποίησης της βάσης δεδομένων NVD. **Ερευνητής-Εισηγητής:** Παναγιώτης Μπουντάκας
56.	**Calculation of the severity and impact of jailbreak and prompt injection attacks in LLMs. (This thesis can be assigned to 2 students)**	ENG: In this thesis, jailbreak and prompt-injection attacks should be executed in an LLM application (e.g., ChatBot operating in an Important NIS 2 sector without guardrails in place - feel free to choose the application and sector). The focus of this thesis should be (i) the definition and categorization of jailbreak and prompt-injection attacks (the dataset can be provided), (ii) the creation of a web-based application for the execution of the malicious prompts to a target LLM application through an API, (iii) the calculation of the severity of the executed attacks (the Artificial Intelligence Vulnerability Scoring System-AIVSS framework can be used: https://aivss.owasp.org/). At

		least 10 jailbreak and 10 prompt injection attacks (considering both direct and indirect) should be executed belonging to different categories. Areas: LLM Security, AIVSS, Prompt Injection, Jailbreak Expected result: (i) creation of a basic chatbot application, (ii) delivery of a script-based application for the generation and execution of the jailbreak and prompt injection prompts, and (iii) calculation of the severity of each generated prompt considering the target GR: Σε αυτή τη διπλωματική εργασία θα πρέπει να εκτελεστούν επιθέσεις jailbreak και prompt-injection σε μια εφαρμογή LLM (π.χ. ChatBot που λειτουργεί σε έναν σημαντικό τομέα του NIS 2 χωρίς την ύπαρξη guardrails - μπορείτε να επιλέξετε ελεύθερα την εφαρμογή και τον τομέα). Η εργασία θα πρέπει να επικεντρωθεί: (i) στον ορισμό και την κατηγοριοποίηση επιθέσεων jailbreak και prompt-injection (το dataset μπορεί να παραχωρηθεί), (ii) στη δημιουργία μιας διαδικτυακής εφαρμογής για την εκτέλεση κακόβουλων prompts προς μια στοχευμένη εφαρμογή LLM μέσω API, (iii) στον υπολογισμό της σοβαρότητας των εκτελεσμένων επιθέσεων (μπορεί να χρησιμοποιηθεί το framework Artificial Intelligence Vulnerability Scoring System-AIVSS: https://aivss.owasp.org/). Θα πρέπει να εκτελεστούν τουλάχιστον 10 επιθέσεις jailbreak και 10 επιθέσεις prompt injection (λαμβάνοντας υπόψη τόσο direct and indirect prompt injections), οι οποίες να ανήκουν σε διαφορετικές κατηγορίες. Τομείς: LLM Security, AIVSS, Prompt Injection, Jailbreak

		Αναμενόμενο αποτέλεσμα: (i) δημιουργία μιας βασικής εφαρμογής chatbot, (ii) παράδοση μιας εφαρμογής βασισμένης σε scripts για τη δημιουργία και εκτέλεση των prompts τύπου jailbreak και prompt injection, και (iii) υπολογισμός της σοβαρότητας κάθε παραγόμενου prompt, λαμβάνοντας υπόψη τον στόχο. **Ερευνητής-Εισηγητής:** Παναγιώτης Μπουντάκας
57.	**Analysis of threats and attacks in agentic AI environments and mitigation measures. (This thesis can be assigned to 2 students)**	ENG: Threat landscape analysis and review of attacks in agentic AI systems focusing on systems where AI Agents interact with external tools or other AI agents. The analysis should consider protocols such as Model Context Protocol (MCP) and Agent-to-Agent (A2A). One attack should be selected and implemented while also analyzing the actions that can lead to the detection of the attack and documented as mitigation actions. Areas: AI agents security, MCP, A2A, mitigation of attacks on AI agents Expected result: (i) A taxonomy of the threat landscape of AI agents, (ii) the representation of an attack, and (ii) the documentation of the mitigation steps. GR: Ανάλυση του πεδίου απειλών και επισκόπηση επιθέσεων σε συστήματα agentic AI, με έμφαση σε συστήματα όπου AI Agents αλληλεπιδρούν με εξωτερικά εργαλεία ή με άλλους AI agents. Η ανάλυση θα πρέπει να λάβει υπόψη πρωτόκολλα όπως το Model Context Protocol (MCP) και το Agent-to-Agent (A2A). Θα πρέπει να επιλεγεί και να υλοποιηθεί μία επίθεση, ενώ παράλληλα να αναλυθούν οι ενέργειες που μπορούν να οδηγήσουν στον

		εντοπισμό της επίθεσης και να καταγραφούν ως ενέργειες μετριασμού (mitigation actions). Τομείς: AI agents security, MCP, A2A, μετριασμός επιθέσεων σε AI agents Αναμενόμενο αποτέλεσμα: (i) μια ταξινομία του τοπίου απειλών των AI agents, (ii) η αναπαράσταση μιας επίθεσης και (iii) η τεκμηρίωση των βημάτων μετριασμού. **Ερευνητής-Εισηγητής:** Παναγιώτης Μπουντάκας
58.	**Analysis of the adversarial threat landscape of AI systems and definition of mitigation actions per threat category**	ENG: This thesis should focus on the definition of the threat categories targeting AI systems (using well-known repositories, such as MITRE Atlas, OWASP Top-10 for LLM, Agentic AI & AI security), analyze their main traits and define mitigation actions that can lead to their mitigation. Given that several threat sources exist (MITRE Atlas, OWASP Top-10) the main focus should be on the identification of the most important traits that can lead to their detection and the identification of the mitigation actions per category. Areas: Threat landscape of AI systems and AI Agents Expected result: creation of a threat taxonomy of AI systems (including AI agents and Agentic AI), analysis of their most important traits, and definition of mitigation actions per threat. GR: Αυτή η διπλωματική εργασία θα πρέπει να επικεντρωθεί στον ορισμό των κατηγοριών απειλών που στοχεύουν συστήματα AI (χρησιμοποιώντας γνωστά αποθετήρια, όπως τα MITRE Atlas, OWASP Top-10 for LLM, Agentic AI

		& AI Security), στην ανάλυση των βασικών χαρακτηριστικών τους και στον καθορισμό ενεργειών μετριασμού που μπορούν να οδηγήσουν στον περιορισμό τους. Δεδομένου ότι υπάρχουν πολλές πηγές απειλών (MITRE Atlas, OWASP Top-10), η κύρια έμφαση θα πρέπει να δοθεί στον εντοπισμό των σημαντικότερων χαρακτηριστικών που μπορούν να οδηγήσουν στην ανίχνευσή τους, καθώς και στον προσδιορισμό των κατάλληλων ενεργειών μετριασμού για κάθε κατηγορία. Τομείς: πεδίο απειλών AI systems και AI Agents Αναμενόμενο αποτέλεσμα: δημιουργία μιας ταξινομίας απειλών για συστήματα AI (συμπεριλαμβανομένων AI agents και Agentic AI), ανάλυση των σημαντικότερων χαρακτηριστικών τους και καθορισμός ενεργειών μετριασμού για κάθε απειλή **Ερευνητής-Εισηγητής:** Παναγιώτης Μπουντάκας
59.	**Security Evaluation and Hardening of RAG-Based Cybersecurity Assistants against Knowledge-Base Poisoning and Indirect Prompt Injection**	Η εργασία θα εστιάσει στην αξιολόγηση της ασφάλειας συστημάτων Retrieval-Augmented Generation που χρησιμοποιούνται ως cybersecurity assistants. Θα μελετηθούν επιθέσεις όπως knowledge-base poisoning, indirect prompt injection, malicious document chunks και retrieval manipulation σε vector databases. Η μεθοδολογία θα περιλαμβάνει ανάπτυξη ενός μικρού RAG prototype, δημιουργία benign και malicious document corpus, εκτέλεση επιθέσεων και αξιολόγηση με μετρικές όπως attack success rate, retrieval contamination rate, answer faithfulness και leakage rate. Αναμενόμενο αποτέλεσμα: ανάπτυξη prototype RAG security evaluation framework, με attack scenarios, evaluation scripts και

		προτεινόμενους μηχανισμούς mitigation, όπως source validation, context isolation και provenance-aware answer generation. **Ερευνητής-Εισηγητής:** Βάιος Μπολγούρας
60.	**Confidential and Verifiable AI Inference for Cybersecurity Applications using Trusted Execution Environments and Remote Attestation**	Η εργασία θα μελετήσει πώς μπορούν να εκτελούνται AI-based cybersecurity services σε περιβάλλοντα εμπιστευτικής εκτέλεσης, με στόχο την προστασία των δεδομένων εισόδου, του μοντέλου και των παραγόμενων αποτελεσμάτων. Θα εξεταστούν τεχνικές Trusted Execution Environments και remote attestation για την παραγωγή evidence ότι ένα AI μοντέλο εκτελέστηκε σε αξιόπιστο περιβάλλον και χωρίς μη εξουσιοδοτημένη τροποποίηση. Η μεθοδολογία θα περιλαμβάνει βιβλιογραφική ανασκόπηση, σχεδίαση αρχιτεκτονικής, ανάπτυξη prototype ή simulated testbed και αξιολόγηση ως προς confidentiality, integrity evidence και performance overhead. Αναμενόμενο αποτέλεσμα: prototype ή technical framework για confidential and verifiable AI inference σε cybersecurity use case, με sample attestation evidence και τεχνική αξιολόγηση. **Ερευνητής-Εισηγητής:** Βάιος Μπολγούρας
61.	**Automated NIS2 Incident Reporting and Evidence Packaging from SOC Alerts using STIX 2.1 and LLM-Assisted Summarisation**	Η εργασία θα εστιάσει στη σχεδίαση και ανάπτυξη ενός μηχανισμού που μετατρέπει security alerts, logs, CTI indicators και analyst notes σε δομημένο πακέτο αναφοράς περιστατικού, κατάλληλο για SOC/CSIRT workflows και υποστήριξη διαδικασιών NIS2 incident reporting. Η μεθοδολογία θα περιλαμβάνει ανάλυση των πληροφοριών που απαιτούνται σε ένα incident report, μοντελοποίηση τεχνικών στοιχείων με STIX 2.1, παραγωγή timeline, affected assets, indicators, severity estimation και recommended response actions. Θα διερευνηθεί επίσης η χρήση LLM-assisted summarisation με

		traceability προς τα αρχικά evidence. Αναμενόμενο αποτέλεσμα: prototype incident evidence packaging and reporting assistant, με sample incident datasets, STIX-based representation, report templates και αξιολόγηση ως προς πληρότητα, ακρίβεια και χρησιμότητα. **Ερευνητής-Εισηγητής:** Βάιος Μπολγούρας
62.	**Vulnerability analysis of binary/executable files with LLMs**	**Θεματική Περιοχή:** Vulnerability assessment, LLM-security, Reverse engineering **Μεθοδολογία:** Στόχος της εργασίας είναι η ανάλυση ευπαθειών σε εκτελέσιμα αρχεία με τη χρήση LLM. Η εργασία επικεντρώνεται στην χρήση αντίστροφης μηχανικής με σκοπό την εξαγωγή του πηγαίου κώδικα, στην ανάλυση του από LLM και τέλος στην δημιουργία αναφοράς που συνδέονται με τα ευρήματα Επομένως, ο διαχωρισμός γίνεται σε τρία διακριτά στάδια: ● Reverse engineering εκτελέσιμων αρχείων με σκοπό την εξαγωγή του πηγαίου κώδικα. ● Ανάλυση του παραγόμενου κώδικα με LLM για τον εντοπισμό πιθανών ευπαθειών και αδυναμιών ασφαλείας. ● Δημιουργία αναφοράς ευρημάτων σε προκαθορισμένο format που συνδέει τα αποτελέσματα της ανάλυσης με τις εντοπισμένες ευπάθειες. **Αναμενόμενο αποτέλεσμα:** Το αναμενόμενο αποτέλεσμα είναι η ανάπτυξη μιας πλήρους λειτουργικής μεθοδολογίας για την ανάλυση ευπαθειών σε εκτελέσιμα αρχεία με τη χρήση LLM. Επίσης, θα περιλαμβάνει την εξαγωγή

		κώδικα μέσω reverse engineering, την αξιολόγηση του κώδικα από το LLM για τον εντοπισμό πιθανών αδυναμιών ασφαλείας και τη δημιουργία δομημένης αναφοράς ευρημάτων σε προκαθορισμένο format. Η αναφορά θα παρουσιάζει τις εντοπισμένες ευπάθειες, τη σοβαρότητά τους και τη σύνδεσή τους με τα αντίστοιχα τμήματα του κώδικα. Επίσης, τα ευρήματα θα πρέπει να περιλαμβάνουν λειτουργικό proof-of-concept κώδικα ώστε να διαπιστωθεί το exploitability της ευπάθειας, καθώς και το αντίστοιχο mitigation. **Ερευνητής-Εισηγητής:** Γιαπαντζής Κωνσταντίνος
63.	**LLM-based web application penetration testing**	**Θεματική Περιοχή:** Penetration testing, Web application security, LLM-security **Μεθοδολογία:** Στόχος της διπλωματικής εργασίας είναι η ανάπτυξη μιας μεθοδολογίας για την αξιοποίηση LLM στη διαδικασία ελέγχου διείσδυσης διαδικτυακών εφαρμογών. Η εργασία εστιάζει στην υποστήριξη επιμέρους σταδίων του penetration testing, όπως η αναγνώριση στόχου, η ανάλυση πιθανών ευπαθειών, η δημιουργία προτάσεων ελέγχου και η παραγωγή δομημένων αναφορών ευρημάτων. Σκοπός είναι η αξιολόγηση του βαθμού στον οποίο τα LLMs μπορούν να ενισχύσουν την αποδοτικότητα, την ακρίβεια και την αυτοματοποίηση της διαδικασίας ελέγχου ασφάλειας web εφαρμογών. Επομένως ο διαχωρισμός γίνεται σε τρία διακριτά στάδια: ● Αναγνώριση και συλλογή πληροφοριών για τη διαδικτυακή εφαρμογή, με στόχο τον εντοπισμό πιθανών σημείων ενδιαφέροντος για έλεγχο ασφάλειας.

		• Ανάλυση πιθανών ευπαθειών με χρήση LLM, αξιοποιώντας τα δεδομένα που συλλέχθηκαν για την υποστήριξη της διαδικασίας penetration testing. • Δημιουργία δομημένης αναφοράς ευρημάτων, η οποία θα παρουσιάζει τα αποτελέσματα του ελέγχου, τις εντοπισμένες αδυναμίες και πιθανές προτάσεις αντιμετώπισης. **Αναμενόμενο αποτέλεσμα:** Το αναμενόμενο αποτέλεσμα είναι η ανάπτυξη μιας μεθοδολογίας για την ενίσχυση του web application penetration testing με τη χρήση LLMs. Η εργασία θα οδηγεί στη συλλογή και ανάλυση πληροφοριών από τη διαδικτυακή εφαρμογή, στον εντοπισμό πιθανών ευπαθειών με τη συνδρομή LLM και στη δημιουργία δομημένης αναφοράς. Η αναφορά θα περιλαμβάνει τις εντοπισμένες αδυναμίες, την αξιολόγηση της σοβαρότητας, λειτουργικό proof-of-concept κώδικα ώστε να διαπιστωθεί το exploitability κάθε ευπάθειας, καθώς και προτάσεις αντιμετώπισης. **Ερευνητής-Εισηγητής:** Γιαπαντζής Κωνσταντίνος
64.	**Evaluation of Self-Sovereign Identity Agents with Post-Quantum Cryptographic Signatures**	**Θεματική Περιοχή:** Μετα-κβαντική Κρυπτογραφία (Post-Quantum Cryptography), Self-Sovereign Identity (SSI), Ψηφιακές Υπογραφές. **Περιγραφή/Μεθοδολογία:** Η εργασία επικεντρώνεται στην ενσωμάτωση και αξιολόγηση μετα-κβαντικών κρυπτογραφικών αλγορίθμων σε αποκεντρωμένες (decentralized) υποδομές Self-Sovereign Identity. Η μεθοδολογία περιλαμβάνει την υλοποίηση ενός υβριδικού σχήματος ψηφιακών υπογραφών (π.χ. συνδυασμός κλασικών υπογραφών ECDSA με lattice-based αλγορίθμους όπως το ML-DSA/Dilithium) εντός ενός SSI agent/wallet. Θα αναλυθεί η χρήση τους σε Decentralized Identifiers (DIDs)

		και Verifiable Credentials (VCs). Στη συνέχεια, θα πραγματοποιηθεί πειραματική δοκιμή και συγκριτική αξιολόγηση με βάση την καθυστέρηση (latency) στο authentication, το μέγεθος των παραγόμενων κλειδιών, και το υπολογιστικό overhead. **Βήματα Υλοποίησης:** 1. Βιβλιογραφική ανασκόπηση των προτύπων Self-Sovereign Identity (DIDs, VCs) και των επικείμενων προτύπων Μετα-κβαντικής Κρυπτογραφίας (π.χ. NIST ML-DSA, ML-KEM). 2. Σχεδιασμός και ανάπτυξη ενός υβριδικού κρυπτογραφικού σχήματος που θα συνδυάζει κλασικές (π.χ. ECDSA) και post-quantum ψηφιακές υπογραφές για ενσωμάτωση σε έναν πρωτότυπο SSI agent. 3. Δημιουργία πειραματικού testbed για την προσομοίωση της ροής έκδοσης (issuance), αποθήκευσης και επαλήθευσης (verification) Verifiable Credentials. 4. Εκτέλεση μετρήσεων απόδοσης (latency, computational overhead, μεγέθη κλειδιών/υπογραφών) και διατύπωση συγκεκριμένων προτάσεων μετριασμού (mitigation) για την αντιμετώπιση του αυξημένου όγκου δεδομένων στα δίκτυα SSI **Ερευνητής-Εισηγητής:** Ιωαννιδης Θεοδωρος
65.	**Adaptive AI Systems and Learner Models for Next-Gen Learning Platforms**	**Θεματική Περιοχή:** Adaptive Learning, Educational AI, Learner Modeling, Generative AI.

		Περιγραφή/Μεθοδολογία: Η εργασία θα μελετήσει τον σχεδιασμό και την ανάπτυξη ενός προσαρμοστικού συστήματος τεχνητής νοημοσύνης (adaptive AI) για πλατφόρμες μάθησης επόμενης γενιάς (π.χ. σύγχρονα LMS). Η μεθοδολογία περιλαμβάνει τη χρήση Large Language Models (LLMs) για τη δυναμική προσαρμογή του εκπαιδευτικού υλικού, του ρυθμού και των μονοπατιών μάθησης, βάσει δεδομένων και προφίλ των εκπαιδευόμενων σε πραγματικό χρόνο (learner profiling, π.χ. μέσω του μοντέλου Felder-Silverman). Θα σχεδιαστεί ένα pipeline παραγωγής προσωποποιημένου πολυμεσικού περιεχομένου (π.χ. στοχευμένα quizzes, προσαρμοσμένες σημειώσεις, alternative explanations) και θα οριστεί πρωτόκολλο αξιολόγησης για την ανάλυση της αλληλεπίδρασης. **Βήματα Υλοποίησης:** 1. Μελέτη μεθοδολογιών ανάλυσης μαθησιακού προφίλ (π.χ. Felder-Silverman) και διερεύνηση των δυνατοτήτων των Large Language Models (LLMs) στην παραγωγή εκπαιδευτικού υλικού. 2. Σχεδιασμός ενός δυναμικού μοντέλου (learner model) που θα συλλέγει και θα αναλύει δεδομένα αλληλεπίδρασης του εκπαιδευόμενου σε πραγματικό χρόνο, εξάγοντας συμπεράσματα για τον ρυθμό και το στυλ μάθησής του. 3. Ανάπτυξη πρωτοτύπου AI module (π.χ. με χρήση API διασύνδεσης LLM) ικανού να παράγει και να αναπροσαρμόζει αυτόματα προσωποποιημένο εκπαιδευτικό περιεχόμενο (όπως επεξηγήσεις και δυναμικά quizzes).

		4. Πιλοτική αξιολόγηση του πρωτοτύπου για τη μέτρηση της χρηστικότητας, της ορθότητας του παραγόμενου περιεχομένου και της συνολικής διατήρησης του ενδιαφέροντος (engagement) του χρήστη. **Ερευνητής-Εισηγητής:** Ιωαννιδης Θεοδωρος
66.	**OpenID-Based Identity Solutions in Gamified Learning Management Systems**	**Θεματική Περιοχή:** Digital Identity, OpenID Connect (OIDC), Gamification, Cybersecurity Education. **Περιγραφή/Μεθοδολογία:** Η εργασία θα διερευνήσει την ενσωμάτωση του προτύπου OpenID Connect (OIDC) σε gamified Συστήματα Διαχείρισης Μάθησης (LMS). Η μεθοδολογία περιλαμβάνει τη χρήση του OIDC για Single Sign-On (SSO) και διαχείριση προφίλ, επιτρέποντας την ασφαλή ταυτοποίηση των εκπαιδευόμενων μέσω ενός κεντρικού Identity Provider (IdP). Θα σχεδιαστεί ένα proof-of-concept (PoC) όπου οι χρήστες συνδέονται με ασφάλεια, εκτελούν εκπαιδευτικά σενάρια κυβερνοασφάλειας, και τα επιτεύγματά τους (badges, πόντοι εμπειρίας) αποθηκεύονται και διαχειρίζονται μέσω δυναμικών OIDC claims ή συνδεδεμένων user info endpoints. Η προσέγγιση αυτή θα εξετάσει πώς η ταυτότητα και η πρόοδος μπορούν να συγκεντρωθούν με ασφάλεια σε εκπαιδευτικά περιβάλλοντα. **Βήματα Υλοποιησης:** 1. Βιβλιογραφική ανασκόπηση του προτύπου OpenID Connect (OIDC), των βασικών ροών αυθεντικοποίησης (authorization code flow) και της χρήσης JSON Web Tokens (JWT) στην εκπαίδευση.

		2. Σχεδιασμός αρχιτεκτονικής διασύνδεσης ενός gamified LMS (Cybergame) με έναν κεντρικό Identity Provider (π.χ. Keycloak, Authentik) για την υλοποίηση Single Sign-On (SSO). 3. Υλοποίηση ενός proof-of-concept (PoC) όπου ο χρήστης αλληλεπιδρά με gamified σενάρια και τα ακαδημαϊκά του επιτεύγματα (badges, scores) ενσωματώνονται δυναμικά στο ταυτοποιημένο προφίλ του μέσω custom OIDC claims ή REST APIs. 4. Αξιολόγηση του συστήματος ως προς την ασφάλεια (π.χ. προστασία των token, ελάχιστα προνόμια), τη διαλειτουργικότητα και τη βελτίωση της συνολικής εμπειρίας χρήστη (UX) κατά τη σύνδεση και τη συλλογή επιτευγμάτων. **Ερευνητής-Εισηγητής:** Ιωαννιδης Θεοδωρος
67.	**Μελέτη επιθέσεων voice cloning**	**Θεματική Περιοχή: Adversarial AI, Voice Cloning** **Περιγραφή:** ● Το θέμα εστιάζει στην ανάλυση επιθέσεων κλωνοποίησης φωνής (voice cloning). Με την έξαρση των παραγωγικών μοντέλων (Generative AI), η δημιουργία ρεαλιστικών φωνών είναι πλέον εφικτή με τη χρήση ελάχιστων δευτερολέπτων ηχητικού δείγματος. Η τεχνολογία αυτή, αν και προσφέρει σημαντικές ευκαιρίες (π.χ. στην ψυχαγωγία ή την προσβασιμότητα), ενέχει σοβαρούς κινδύνους ασφάλειας. **Μεθοδολογία:**

		• Βιβλιογραφική Ανασκόπηση (έρευνα στο τι υπάρχει στην βιβλιογραφία), Μοντελοποίηση Απειλών (ερευνά στα σενάρια επίθεσης), Μελέτη Αντιμέτρων • Σχεδιασμός και υλοποίηση ενδεικτικής επίθεσης με χρήση διαφόρων open-source εργαλείων για τοπική κλωνοποίηση φωνής σε Python/JavaScript, μετρικές και αξιολόγηση αποτελεσμάτων **Αναμενόμενο αποτέλεσμα:** • Υλοποίηση και αποτελέσματα πειραμάτων. **Ερευνητής-Εισηγητής:** Γραμματόπουλος Αθανάσιος
68.	**Hardware and Firmware Emulation CTF Framework**	**Περιγραφή:** • Ανάπτυξη ενός Framework για CTF δοκιμασίες που χρησιμοποιεί εξομοιωτές/προσομοιωτές για να φέρει τους παίκτες αντιμέτωπους με την παραβίαση υλικού ή/και υλικολογισμικού, χωρίς να απαιτείται η χρήση φυσικών συσκευών (πχ FPGA, Arduino, Specific SOCs, custom boards). **Μεθοδολογία:** • Βιβλιογραφική Ανασκόπηση (έρευνα στο τι υπάρχει στην βιβλιογραφία, τι τεχνολογίες μπορούν να χρησιμοποιηθούν, τι εργαλεία υπάρχουν) • Ανάλυση πιθανών σεναρίων ασκήσεων για επιθέσεις σε υλικό ή/και υλικολογισμικό • Δημιουργία εικονικού περιβάλλοντος για την αλληλεπίδραση (πχ με UART/JTAG)

		Αναμενόμενο αποτέλεσμα: ● The developed Framework ● 4 Exercises using the framework **Ερευνητής-Εισηγητής:** Γραμματόπουλος Αθανάσιος
69.	**Ανίχνευση Απειλών σε IoT/OT Περιβάλλοντα Κρίσιμων Υποδομών με Ανάλυση Δικτυακής Συμπεριφοράς και Εξηγήσιμη Τεχνητή Νοημοσύνη**	Η εργασία θα εστιάσει στον σχεδιασμό και την ανάπτυξη ενός μηχανισμού που διασφαλίζει την ακεραιότητα και την ιχνηλασιμότητα κρίσιμων logs σε περιβάλλον κρίσιμης υποδομής. Η τεχνολογική βάση θα είναι **immutable logging**, **hash-based audit trails**, **decentralized ledger technologies** και η σύνδεση των καταγραφών με διαδικασίες forensic analysis και compliance reporting. Η εργασία θα εξετάσει πώς μπορούν να καταγράφονται κρίσιμα γεγονότα, όπως πρόσβαση σε ευαίσθητα δεδομένα, αλλαγές πολιτικών, alerts και ενέργειες απόκρισης, ώστε να είναι επαληθεύσιμα μετά από περιστατικό. **Τελικό αποτέλεσμα**: Ανάπτυξη prototype log integrity service, με schema γεγονότων, μηχανισμό υπολογισμού/επαλήθευσης αποτυπωμάτων, audit trail, βασικά verification queries και αξιολόγηση απόδοσης και ακεραιότητας. **Θεματική Περιοχή**: Immutable Logging, Digital Forensics, Distributed Ledger Technologies, Compliance Evidence, Critical Infrastructure Cybersecurity. **Ερευνητής-Εισηγητής:** Μακροπόδης Ιωάννης
70.	**Σχεδίαση και Ανάπτυξη Πρωτοτύπου SIEM για Παρακολούθηση Συμβάντων Ασφάλειας σε Κρίσιμες Υποδομές**	Η εργασία θα εστιάσει στον σχεδιασμό και την ανάπτυξη ενός πρωτοτύπου **Security Information and Event Management** για κρίσιμες υποδομές. Το σύστημα θα συλλέγει και θα κανονικοποιεί γεγονότα ασφάλειας από διαφορετικές πηγές, όπως συστήματα πρόσβασης, endpoints, δικτυακές

		ροές, εφαρμογές και IoT/OT συσκευές. Η τεχνολογική βάση θα είναι η **log normalization**, η **event correlation**, η **rule-based detection** κα παραγωγή δομημένων alerts**. Τελικό αποτέλεσμα:** Ανάπτυξη Συστήματος / Υπηρεσίας σε μορφή prototype SIEM layer, με μοντέλο εισαγωγής logs, schema κανονικοποίησης, κανόνες συσχέτισης, ενδεικτικά alerts, dashboard ή structured report και τεχνική αξιολόγηση σε συνθετικά σενάρια κρίσιμων υποδομών. **Θεματική Περιοχή**: SIEM, Security Monitoring, Event Correlation, Critical Infrastructure Cybersecurity. **Ερευνητής-Εισηγητής:** Μακροπόδης Ιωάννης
71.	**Σχεδίαση και Ανάπτυξη Πρωτοτύπου SOAR για Αυτοματοποίηση Απόκρισης σε Περιστατικά Κυβερνοασφάλειας**	Η εργασία θα εστιάσει στον σχεδιασμό και την ανάπτυξη ενός πρωτοτύπου Security Orchestration, Automation and Response για την αυτοματοποίηση βασικών ενεργειών απόκρισης σε περιστατικά ασφάλειας. Το πρωτότυπο θα περιλαμβάνει playbooks για συνηθισμένα περιστατικά, όπως phishing, ransomware indication, ύποπτη σύνδεση, πιθανή διαρροή δεδομένων ή ανίχνευση κακόβουλης δικτυακής συμπεριφοράς. Η τεχνολογική βάση θα είναι η incident response automation, η playbook modelling, η case management και η automated escalation. **Τελικό αποτέλεσμα**: Ανάπτυξη prototype SOAR workflow engine, με βιβλιοθήκη playbooks, μοντέλο κατάστασης περιστατικού, αυτοματοποιημένες ενέργειες απόκρισης, structured incident report και αξιολόγηση με βάση χρόνο απόκρισης, πληρότητα ενεργειών και δυνατότητα επανάληψης. **Θεματική Περιοχή**: SOAR, Incident Response Automation, Security Orchestration, Critical Infrastructure Resilience. **Ερευνητής-Εισηγητής:** Μακροπόδης Ιωάννης

72.	**LLM-Based Συμβουλευτικός Μηχανισμός για Κυβερνοασφάλεια και Συμμόρφωση σε Κρίσιμες Υποδομές**	Η εργασία θα εστιάσει στην ανάπτυξη ενός συμβουλευτικού μηχανισμού που χρησιμοποιεί **large language models** και **retrieval-augmented reasoning** για να παρέχει καθοδηγούμενες απαντήσεις σε ερωτήματα κυβερνοασφάλειας, κινδύνου και συμμόρφωσης σε κρίσιμες υποδομές. Η έμφαση θα δοθεί όχι στο εργαλείο, αλλά στην τεχνολογική μεθοδολογία: οντολογίες κυβερνοασφάλειας κρίσιμων υποδομών, έλεγχος αξιοπιστίας απαντήσεων, πολιτικές ασφαλούς χρήσης, explainable recommendations και περιορισμός λανθασμένων ή μη συμμορφούμενων απαντήσεων. **Τελικό αποτέλεσμα**: Ανάπτυξη prototype advisory assistant, με knowledge base, ερωτήματα αξιολόγησης, μηχανισμό τεκμηριωμένης απάντησης, guardrail policy, structured recommendations και αξιολόγηση ακρίβειας/χρησιμότητας σε σενάρια SOC, compliance και risk management. **Θεματική Περιοχή**: Large Language Models, Cybersecurity Advisory Systems, Retrieval-Augmented Generation, AI Governance, Critical Infrastructure Compliance. **Ερευνητής-Εισηγητής:** Μακροπόδης Ιωάννης
73.	**Ορχήστρωση και Αυτοματοποίηση Απόκρισης σε Περιστατικά Ransomware σε Κρίσιμες Υποδομές**	Η εργασία θα εστιάσει στην ανάπτυξη μεθοδολογίας και πρωτοτύπου για την αυτοματοποίηση απόκρισης σε σενάρια ransomware που επηρεάζουν κρίσιμες υπηρεσίες. Η τεχνολογική βάση θα είναι η security orchestration and automated response, με playbooks που περιγράφουν στάδια όπως ανίχνευση, επιβεβαίωση, απομόνωση επηρεαζόμενων συστημάτων, ενημέρωση υπευθύνων, συλλογή τεκμηρίων και υποστήριξη αποκατάστασης**. Τελικό αποτέλεσμα**: Ανάπτυξη prototype incident-response orchestration framework, με βιβλιοθήκη playbooks, μοντέλο κατάστασης περιστατικού, μηχανισμό ενεργοποίησης ενεργειών, structured incident report και αξιολόγηση με βάση χρόνο απόκρισης, πληρότητα ενεργειών και

		δυνατότητα επανάληψης**. Θεματική Περιοχή**: Incident Response Automation, Ransomware Defence, SOAR Technologies, Critical Infrastructure Resilience. **Ερευνητής-Εισηγητής:** Μακροπόδης Ιωάννης

[1] *Στη σύντομη περιγραφή της διπλωματικής εργασίας θα πρέπει να αναφέρεται σαφώς το τελικό αποτέλεσμα αυτής (Εκπόνηση Μελέτης, Ανάπτυξη Συστήματος / Υπηρεσίας, Ανασκόπηση / Συγκριτική Αξιολόγηση, κτλ).*