ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΠΜΣ «**ΔΙΟΙΚΗΣΗ, ΑΝΑΛΥΤΙΚΗ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΕΠΙΧΕΙΡΗΣΕΩΝ**»

Δήλωση Διπλωματικής Εργασίας ή Project – ΕΝΤΥΠΟ Β

(Συμπληρώστε στο σκιασμένο μέρος. Η περιγραφή οφείλει να είναι λιτή και σύντομη)

Διπλωματική Εργασία ή Project
(Υπογραμμίστε την επιλογή σας): PROJECT

Ακαδ. Έτος: 2025 - 2026

Επώνυμο και Όνομα: Λέφας Ηρακλής

Εποπτεύων / Εποπτεύουσα: Θανάσης Αργυρίου
(Είναι απαραίτητο να δηλωθεί)

Ημερομηνία: 24/9/2025

Α. Προτεινόμενος Τίτλος
(Σύντομος και εστιασμένος στο αντικείμενο)
ML utilization in Anomaly Detection for Cybersecurity

Β. Σύντομη Περιγραφή
(Έως 250 λέξεις. Ρητή περιγραφή του προβλήματος και των αποτελεσμάτων ως προς περιεχόμενο, μέθοδο και σημαντικότητα. Πχ μπορείτε να σκεφθείτε σε όρους: αριθμός κεφαλαίων, περιεχόμενο, δεδομένα, αναμενόμενα αποτελέσματα, μέθοδος ανάλυσης)

Σκοπός του Project είναι η εφαρμογή, ανάλυση και σύγκριση διαφόρων αλγορίθμων μηχανικής μάθησης σε κατάλληλο σετ δεδομένων που σχετίζεται με την ανάλυση δεδομένων κυβερνο-επιθέσεων (cybersecurity incidents-attacks).
Θα ήθελα να χρησιμοποιήσω ένα εύρος αλγορίθμων, ενδεχομένως συμπεριλαμβανομένων και ορισμένων που δεν έχουν διδαχθεί (πχ XGBoost) ή που δεν εξετάστηκαν στο πλαίσιο του ΠΜΣ (πχ Neural Networks).
Στοχεύω να χρησιμοποιήσω το Project για να εμβαθύνω και να κατανοήσω περισσότερο τους αλγορίθμους μηχανικής μάθησης, τόσο σε θεωρητικό, όσο και σε πρακτικό πλαίσιο, στο πλαίσιο του επιλεχθέντος πεδίου (Κυβερνοασφάλεια).
Σκοπεύω να εφαρμόσω Data Cleaning, Data Manipulation, Exploratory Data Analysis και τεχνικές Data Visualization, και εφαρμογή Feature Engineering στο επιλεχθέν σετ δεδομένων, με σκοπό την περαιτέρω εφαρμογή και σύγκριση μοντέλων μηχανικής μάθησης.
Θα ήθελα να χρησιμοποιήσω γλώσσα προγραμματισμού Python, καθώς και Version Control με Git και ενδεχομένως σύνδεση με μια Βάση Δεδομένων (εφόσον είναι απαραίτητο).

Γ. 1 Σχετικότητα προς ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ
3 – Ισχυρή, 2- Μέτρια, 1-Ασθενής. Εξηγείστε πολύ σύντομα.
1-Ασθενής

Γ. 2 Σχετικότητα προς ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΕΠΙΧΕΙΡΗΣΕΩΝ
3 – Ισχυρή, 2- Μέτρια, 1-Ασθενής. Εξηγείστε πολύ σύντομα.
1-Ασθενής

Γ. 3 Σχετικότητα προς ΑΝΑΛΥΤΙΚΗ ΕΠΙΧΕΙΡΗΣΕΩΝ, ΕΠΙΣΤΗΜΗ ΔΕΔΟΜΕΝΩΝ
3 – Ισχυρή, 2- Μέτρια, 1-Ασθενής Εξηγείστε πολύ σύντομα.
3 – Ισχυρή, για τους λόγους που αναφέρθηκαν παραπάνω (παρα. Β).

Γ.4 Συνδυασμός των ανωτέρω
(Έως 80 λέξεις)
-
Γ.5 Τίποτε εκ των ανωτέρω
(Έως 80 λέξεις)
-

Δ. ΤΑΞΙΝΟΜΗΣΗ ΘΕΜΑΤΙΚΗΣ ΕΝΟΤΗΤΑΣ
JEL
ή
ACM Computing Classification System (CCS
ή
Mathematics Subject Classification – MSC2020
ή συνδυασμός
ACM Computing Classification System (CCS)

Δ1. ΤΑΞΙΝΟΜΗΣΗ ΘΕΜΑΤΙΚΗΣ ΕΝΟΤΗΤΑΣ: Περιοχή Έρευνας (θεωρία αποφάσεων, οικονομικά, διοίκηση, στρατηγική, πληροφοριακά συστήματα, αναλυτική) **.** (Έως 80 λέξεις)
ΑΝΑΛΥΤΙΚΗ, ΕΠΙΣΤΗΜΗ ΔΕΔΟΜΕΝΩΝ, ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Δ2. ΤΑΞΙΝΟΜΗΣΗ ΘΕΜΑΤΙΚΗΣ ΕΝΟΤΗΤΑΣ: Μεθοδολογία (επισκόπηση, πρωτογενής έρευνα, δευτερογενής έρευνα) **και εργαλεία ανάπτυξης** (επιχειρησιακή έρευνα, παλινδρόμηση, στατιστική, μαθηματικά, κλπ). (Έως 80 λέξεις)
Η Μεθοδολογία περιλαμβάνει επισκόπηση βιβλιογραφίας (ανασκόπηση και ανάλυση της υπάρχουσας βιβλιογραφίας και ανάπτυξη ερευνητικών ερωτημάτων) και Δευτερογενή έρευνα επί ήδη συλλεχθέντων δεδομένων, με σκοπό τη συγκριτική ανάλυση.
Ως εργαλεία ανάπτυξης θα χρησιμοποιηθούν η στατιστική/μαθηματικά, η μηχανική μάθηση, ο προγραμματισμός και στοιχεία Κυβερνοασφάλειας.

Δ3. ΤΑΞΙΝΟΜΗΣΗ ΘΕΜΑΤΙΚΗΣ ΕΝΟΤΗΤΑΣ: Θεματική περιοχή (διοίκηση, πληροφοριακά συστήματα, αναλυτική) (Έως 80 λέξεις)
Επιστήμη Δεδομένων και Αναλυτική

Ε. ΕΡΓΑΛΕΙΑ

Ποια θα είναι η μεθοδολογική προσέγγιση;

Σκοπεύω να εφαρμόσω Data Cleaning, Data Manipulation, Exploratory Data Analysis και τεχνικές Data Visualization και εφαρμογή Feature Engineering στο επιλεχθέν σετ δεδομένων, με σκοπό την περαιτέρω εφαρμογή και σύγκριση μοντέλων μηχανικής μάθησης.

Από που θα αντλήσετε δεδομένα; (Να αναφερθεί το είδος των δεδομένων, η πηγή τους, η διαθεσιμότητα)

Open Source δεδομένα, διαθέσιμα στο διαδίκτυο (Kaggle)

Θα χρησιμοποιήσετε λογισμικό; (Αναφορά στο λογισμικό που θα χρησιμοποιηθεί για την ανάλυση των δεδομένων)

Python, Git

Προκαταρκτική Βιβλιογραφία (μερικές αναφορές)

Adelusola, Michael. *AI-Driven Cybersecurity: A Systematic Review of Current Research and Future Directions*. 1 Apr. 2021, www.researchgate.net/publication/386503794_AI-Driven_Cybersecurity_A_Systematic_Review_of_Current_Research_and_Future_Directions.

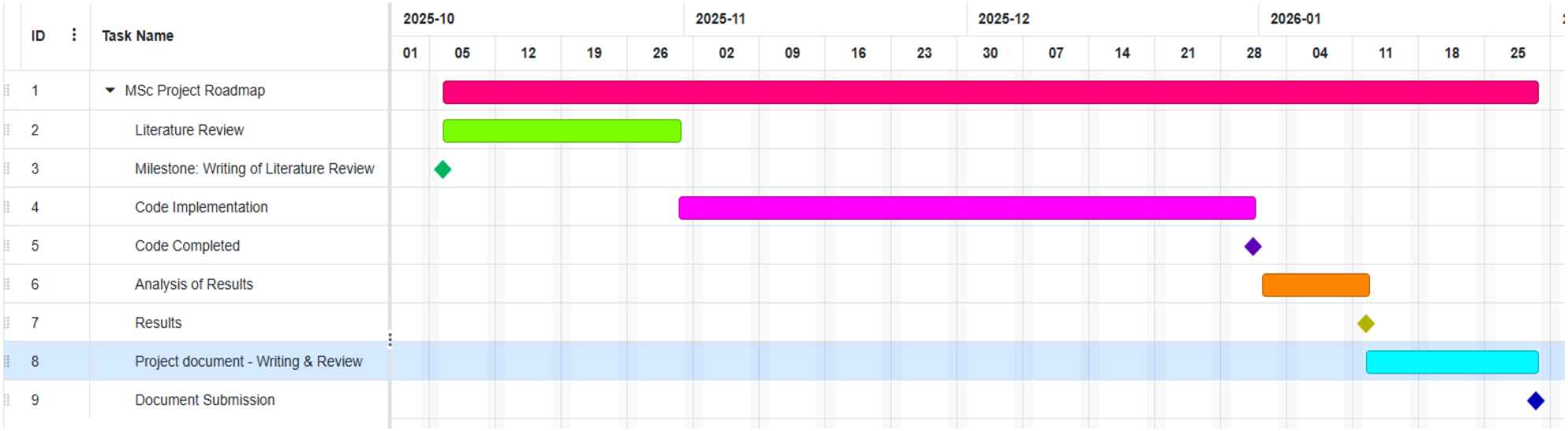
Ali, Sijjad, et al. "AI-Driven Fusion with Cybersecurity: Exploring Current Trends, Advanced Techniques, Future Directions, and Policy Implications for Evolving Paradigms– a Comprehensive Review." *Information Fusion*, vol. 118, 6 Jan. 2025, p. 102922, www.sciencedirect.com/science/article/abs/pii/S1566253524007000, https://doi.org/10.1016/j.inffus.2024.102922.

Kumar Rajaram, Shravan. "AI-Driven Threat Detection: Leveraging Big Data for Advanced Cybersecurity Compliance." *Educational Administration: Theory and Practice*, 18 Nov. 2024, pp. 285–296, https://doi.org/10.53555/kuey.v28i4.7529.

Wiafe, Isaac, et al. "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature." *IEEE Access*, vol. 8, 2020, pp. 146598–146612, https://doi.org/10.1109/access.2020.3013145.

Zeng, Qinghao. *A Comprehensive Review on the Applications of Artificial Intelligence in Cybersecurity*. 7 Mar. 2025, pp. 172–179, https://doi.org/10.1145/3729706.3729732.

Στ. ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΟΛΟΚΛΗΡΩΣΗΣ
(**Συνοπτική παρουσίαση με διάγραμμα GANTT**)



Ζ. Σχόλια από τον ακαδημαϊκό υπεύθυνο
Το θέμα προς ανάλυση είναι επίκαιρο

ΠΡΟΣΟΧΗ

- Το Έντυπο Β οφείλει 1) να έχει όνομα επιβλέποντος και 2) την έγκριση του επιβλέποντος για το θέμα.
- Το Έντυπο Β συνοδεύεται από το Χρονοδιάγραμμα εκπόνησης – είναι στα Έγγραφα του eclass. Η ημερομηνία υποβολής της διπλωματικής / project είναι η 28/2/2026.
- Το Έντυπο Β αναρτάται στο «eclass\Διπλωματική Εργασία\Εργασίες – Έντυπο Β» και υποβάλλεται στη Γραμματεία (bis-analytics@econ.uoa.gr) σε μορφή doc ή Latex ή text k και pdf με ταυτόχρονη κοινοποίηση στον επιβλέποντα.