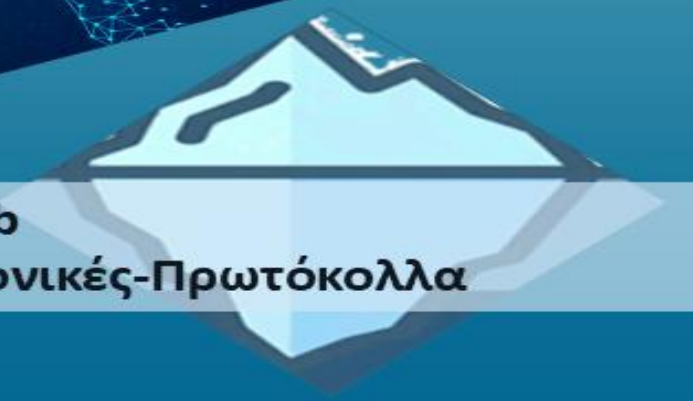
ΣΧΟΛΗ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ηλεκτρόνιο

Τεύχος 4ο

Χρήση Μετασχηματιστών στην Επεξεργασία φυσικής γλώσσας



Dark Web
Χαρακτηριστικά- Αρχιτεκτονικές-Πρωτόκολλα

OpenData: Δυνατότητες και Περιορισμοί

Μέθοδοι δοκιμής λογισμικού και συγκριτική αξιολόγηση τους:

App Invnentor
Ένα εργαλείο για δημιουργική απασχόληση με τις έξυπνες κινητές συσκεύες

ΣΧΟΛΗ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΣΤΡΑΤΟΠΕΔΟ ΖΟΡΜΠΑ
Μεγάλου Αλεξάνδρου 2-4,
Ζωγράφου Αττικής, ΤΚ 15773

ΕΚΔΟΤΗΣ
ΤΜΗΜΑ ΜΕΛΕΤΩΝ ΣΠΗΥ

ΕΠΙΜΕΛΕΙΑ ΣΥΝΤΑΞΗΣ
Σχης (ΠΛΗ-ΕΥ) Γεώργιος Π. Χόντος
Ανχης (ΠΛΗ) Νικόλαος Καλδάνης
Υπχος (Ε) Ασημάκης Κυπριώτης ΠΝ
Ανθστής (ΠΛΗ) Αναστάσιος Σιούτης

ΠΕΡΙΕΧΟΜΕΝΑ

Χαιρετισμός Διοικητή ΣΠΗΥ

Αγαπητοί αναγνώστες,

Με ιδιαίτερη χαρά σας παρουσιάζω το 4ο τεύχος του περιοδικού «ΗΛΕΚΤΡΟΝΙΟ», στο οποίο εξερευνούμε ορισμένες από τις πιο συναρπαστικές και δυναμικά εξελισσόμενες περιοχές της πληροφορικής και της τεχνολογίας. Το περιοδικό διανύοντας το δεύτερο χρόνο κυκλοφορίας του, δεν αποτελεί απλά μια ακόμη έκδοση, αλλά ένα ζωντανό σημείο αναφοράς για την τεχνολογική κοινότητα των Ενόπλων Δυνάμεων. Σε έναν κόσμο όπου οι γραμμές του κώδικα (script code) ορίζουν πλέον τις γραμμές των «μετώπων», η αποστολή μας παραμένει ξεκάθαρη: η μετατροπή της πληροφορίας σε πλεονέκτημα.

Στο συγκεκριμένο τεύχος, οι αρθρογράφοι εστιάζουν στον τρόπο σκέψης που απαιτείται για την αντιμετώπιση των σύγχρονων τεχνολογικών προκλήσεων. Το περιεχόμενο καλύπτει ένα ευρύ φάσμα θεμάτων. Από τις τελευταίες εξελίξεις στην **Επεξεργασία Φυσικής Γλώσσας** και τις αθέατες διαδρομές του **Dark Web**, έως τις δυνατότητες αλλά και τους περιορισμούς των **Ανοιχτών Δεδομένων**. Παράλληλα, παρουσιάζεται μια συγκριτική ανάλυση **Μεθόδων Δοκιμής Λογισμικού**, χρήσιμη για προγραμματιστές και ερευνητές, ενώ η πλατφόρμα **App Inventor** αναδεικνύεται ως ένα δημιουργικό εργαλείο εισαγωγής στον κόσμο των έξυπνων εφαρμογών.

Εύχομαι το παρόν τεύχος να αποτελέσει πηγή έμπνευσης, γνώσης και περαιτέρω αναζήτησης για κάθε αναγνώστη.

Με εκτίμηση

Συνταγματάρχης (ΠΛΗ-ΕΥ) Γεώργιος Π. Χόντος
Διοικητής ΣΠΗΥ

Σημείωμα Έκδοσης

Στην εποχή της ταχύτητας και της διαρκούς ψηφιακής επέκτασης, η ικανότητα να σκέφτεται κανείς κριτικά είναι η πιο σημαντική δεξιότητα. Το τέταρτο τεύχος του περιοδικού ευελπιστεί να αποτελέσει έναν οδηγό για τον τρόπο σκέψης που απαιτείται για την κατανόηση και την αντιμετώπιση των σημερινών προκλήσεων. Έχουν επιλεγεί άρθρα που αναλύουν καίρια θέματα, καλύπτοντας ένα ευρύ φάσμα από τον πυρήνα της Τεχνητής Νοημοσύνης έως τις πρακτικές εφαρμογές της ανάπτυξης λογισμικού:

- **Χρήση Μετασχηματιστών στην επεξεργασία Φυσικής Γλώσσας**: Εμβαθύνουμε στους αλγορίθμους που βρίσκονται πίσω από τα σύγχρονα γλωσσικά μοντέλα (NLP), αναλύοντας την τεχνολογία των Μετασχηματιστών που οδήγησε στην επανάσταση της Τεχνητής Νοημοσύνης.

- **Dark Web**: Μια αναλυτική ματιά, εξετάζοντας τα δομικά στοιχεία (αρχιτεκτονικές και πρωτόκολλα) και τα ιδιαίτερα χαρακτηριστικά του, προκειμένου να κατανοήσουμε τις αθέατες ψηφιακές διαδρομές.

- **Open Data**: Διευρύνουμε τη δύναμη των Ανοιχτών Δεδομένων, αναδεικνύοντας τις τεράστιες δυνατότητες για διαφάνεια και καινοτομία, αλλά παράλληλα θέτοντας τα όρια και τις προκλήσεις στη διαχείρισή τους.

- **Μέθοδοι δοκιμής λογισμικού** και συγκριτική αξιολόγηση τους: Συγκρίνουμε και αναλύουμε των κρίσιμων μεθόδων δοκιμής λογισμικού, με στόχο τη διασφάλιση της ποιότητας.

- **App Invnentor**: Παρουσιάζουμε μια δημιουργική πύλη για την εισαγωγή στην ανάπτυξη εφαρμογών για έξυπνες συσκευές, τονίζοντας τη σημασία της πρακτικής εξάσκησης και της εφευρετικότητας.

Χρήση Μετασχηματιστών στην Επεξεργασία Φυσικής Γλώσσας

Σχης (ΠΛΗ) Δημήτριος Ντόντος.

Εισαγωγή

Στη σύγχρονη εποχή η διεξαγωγή του πολέμου δεν περιορίζεται στα συμβατικά πεδία μαχών. Οι πολεμικές συγκρούσεις αποκτούν υβριδικές μορφές, καθιστώντας την πληροφορία όλο και πιο σημαντική για την έκβαση τους. Ο υβριδικός πόλεμος συνδυάζει στρατιωτικά, διπλωματικά, οικονομικά και πληροφοριακά μέσα για την επίτευξη στρατηγικών στόχων [1].

Στο πλαίσιο αυτό, η παραπληροφόρηση και η προπαγάνδα χρησιμοποιούνται σε συγκρούσεις, πολιτικές κρίσεις και στρατιωτικές επιχειρήσεις. Στο πληροφοριακό πεδίο, η προπαγάνδα χρησιμοποιείται για:

- Διαμόρφωση της κοινής γνώμης υπέρ ή κατά ενός δρώντα.
- Αποπροσανατολισμό ή σύγχυση των αντίπαλων δυνάμεων.
- Δημιουργία κοινωνικής αστάθειας μέσω πόλωσης και διασποράς φόβου.

Οι ψυχολογικές επιχειρήσεις (Psy Ops) και οι επιχειρήσεις επιρροής (Influence Operations) χρησιμοποιούν συστηματικά την τεχνολογία για τη διανομή προπαγανδιστικών περιεχομένων. Ο βαθμός επιτυχίας τους είναι καθοριστικός για την απόδοση συγκριτικού πλεονεκτήματος. Από τη άλλη πλευρά, η ικανότητα ταχείας και ακριβούς ανίχνευσης τέτοιων πληροφοριακών απειλών, είναι ο βασικότερος τρόπος αντιμετώπισης τους. Οι σύγχρονες μεθοδολογίες επεξεργασίας φυσικής γλώσσας [Natural Language Processing (NLP)], παρέχουν σημαντικά και αποτελεσματικά εργαλεία για τη γρήγορη επεξεργασία και ανάλυση μεγάλων όγκων κειμένων (συχνά προερχομένων από ανοικτές Διαδικτυακές πηγές όπως μέσα κοινωνικής δικτύωσης, ειδησεογραφικούς δικτυακούς τόπους και πλατφόρμες συζητήσεων) [2].

Η Επεξεργασία Φυσικής Γλώσσας (NLP) είναι ένας τρόπος ανάλυσης κειμένων με ηλεκτρονικά μέσα και περιλαμβάνει τη συλλογή γνώσεων σχετικά με τον τρόπο με τον οποίο οι άνθρωποι κατανοούν και χρησιμοποιούν τη γλώσσα. Αυτό γίνεται με σκοπό την ανάπτυξη κατάλληλων εργαλείων και τεχνικών που θα μπορούσαν να κάνουν τα συστήματα υπολογιστών να κατανοούν και να χειρίζονται τις φυσικές γλώσσες για την εκτέλεση διαφόρων επιθυμητών εργασιών [3].

Περιλαμβάνει ένα ευρύ σύνολο υπολογιστικών τεχνικών για την ανάλυση και την αναπαράσταση κειμένων γραμμένων σε φυσική γλώσσα. Η ανάλυση αυτή πραγματοποιείται σε ένα ή περισσότερα επίπεδα γλωσσικής ανάλυσης και βασίζεται στη λειτουργία στοιχείων λογισμικού και υλικού υπολογιστικών συστημάτων [4].

Η γενική διαδικασία επεξεργασίας φυσικής γλώσσας περιλαμβάνει τα ακόλουθα στάδια:

- Εντοπισμός των προτάσεων (Sentence segmentation): Η διεργασία ορισμού των προτάσεων από τις οποίες αποτελείται το κείμενο.

- Εντοπισμός των λέξεων (Word tokenization): Κάθε πρόταση αναλύεται σε λέξεις και γλωσσικά μόρια.

- Κανονικοποίηση των λέξεων (Stemming): Οι λέξεις μπορεί να περιλαμβάνονται πολλές φορές σε ένα κείμενο με διαφορετικές μορφές. Σε όλες τους τις εμφανίσεις αντιστοιχίζονται σε μία κοινή μορφή τους (συνήθως στη ρίζα τους).

- Λημματοποίηση (Lemmatization): Αντιστοιχίζεται σε κάθε λέξη η κανονική της μορφή (ανεξάρτητα σε ποιο μέρος του λόγου είναι γραμμένη ή οποιαδήποτε μορφή μπορεί να έχει).

- Απομάκρυνση λέξεων που δεν παρέχουν πληροφορία για την ερμηνεία του κειμένου (stop words). Αυτές οι λέξεις είναι προκαθορισμένες για κάθε γλώσσα (πχ οι λέξεις «είναι», «και», «το», «ή»)

- Αναζήτηση και ανάλυση εξαρτήσεων (Dependency Parsing): Αναζητείται η συσχέτιση των λέξεων που περιλαμβάνονται στις προτάσεις.

- Καθορισμός του μέρους του λόγου που ανήκει κάθε λέξη (Part-of-speech tagging) [5].

Τα τελευταία χρόνια, ραγδαία ανάπτυξη των τεχνολογιών της πληροφορικής στον τομέα της Τεχνητής Νοημοσύνης, οδήγησε στην παρουσίαση αποδοτικών μεθοδολογιών τεχνολογιών επεξεργασίας φυσικής γλώσσας, ενώ και η σχετική ακαδημαϊκή έρευνα παρουσιάζει υψηλή δυναμική. Μια τέτοια μεθοδολογία είναι και η χρήση των Μετασχηματιστών (Transformers) [6].

Στο παρόν άρθρο επιχειρείται μία συνοπτική παρουσίαση της λειτουργίας των Μετασχηματιστών, με έμφαση στη χρήση τους σε εργασίες κατηγοριοποίησης.

Μετασχηματιστές (Transformers)

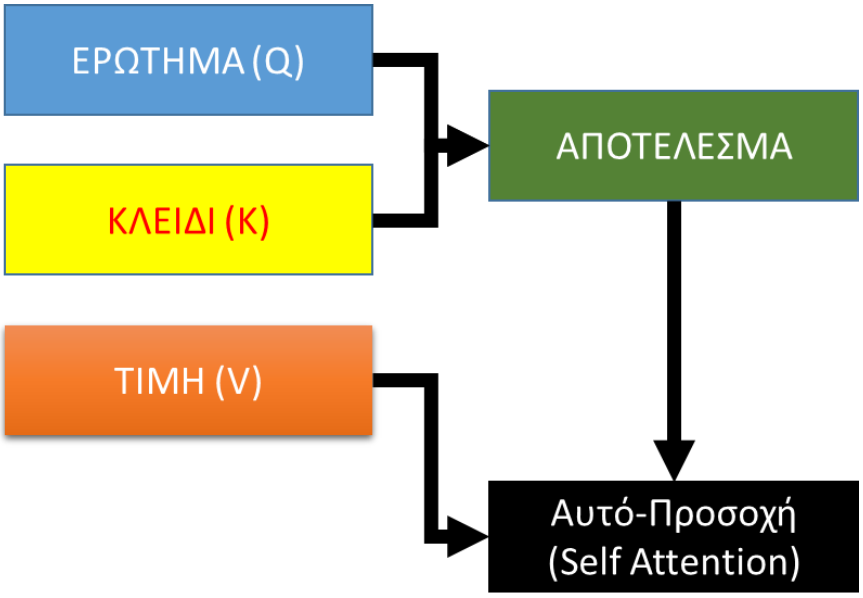
Οι Μετασχηματιστές είναι αρχιτεκτονικές νευρωνικών δικτύων που χρησιμοποιούνται για την αναπαράσταση της πληροφορίας που εμπεριέχεται σε ένα γλωσσικό σύνολο (π.χ. μία πρόταση) [7]. Η πληροφορία αυτή περιλαμβάνει το σύνολο των λέξεων που εμφανίζονται, τη θέση τους και τη μεταξύ τους σχέση.

Βασικό τους πλεονέκτημα είναι το ότι ολοκληρώνουν τη διαδικασία της εκπαίδευσης ταχύτερα και επιτρέπουν αποδοτική παραλληλοποίηση στις GPU[1].

Οι μετασχηματιστές λειτουργούν με δεδομένα ακολουθίας. Λαμβάνουν μια ακολουθία εισόδου και μετά την επεξεργασία της, δίνουν στην έξοδο μια άλλη ακολουθία. Κύριος μηχανισμός των Μετασχηματιστών είναι η αυτό-προσοχή (self-attention). Βασίζεται στην ιδέα ότι σε ένα μεγάλο τμήμα κειμένου, το μεγαλύτερο μέρος της ωφέλιμης πληροφορίας, βρίσκεται σε ένα μικρό μέρος των στοιχείων του.

Οι μηχανισμοί αυτο-προσοχής επιτρέπουν στους Μετασχηματιστές να διατηρούν μεγάλα μέρη των κειμένων στην μνήμη τους (μεγαλύτερα από άλλες μορφές νευρωνικών δικτύων όπως τα RNN και τα LSTM-RNN) και να μπορούν έτσι να συσχετίζουν τμήματα τους, που βρίσκονται σε μεγάλη απόσταση μεταξύ τους [8].

Λειτουργούν υπολογίζοντας σταθμισμένες συσχετίσεις μεταξύ όλων των ζευγών στοιχείων της εισόδου. Η είσοδος αναλύεται σε τρία μέρη: ερωτήματα (Q), κλειδιά (K) και τιμές (V). Το ζητούμενο είναι να αξιολογηθεί ο βαθμός συσχέτισης του ερωτήματος με το κλειδί, προκειμένου να εντοπιστούν τα κυριότερα σημεία της εισόδου [7].



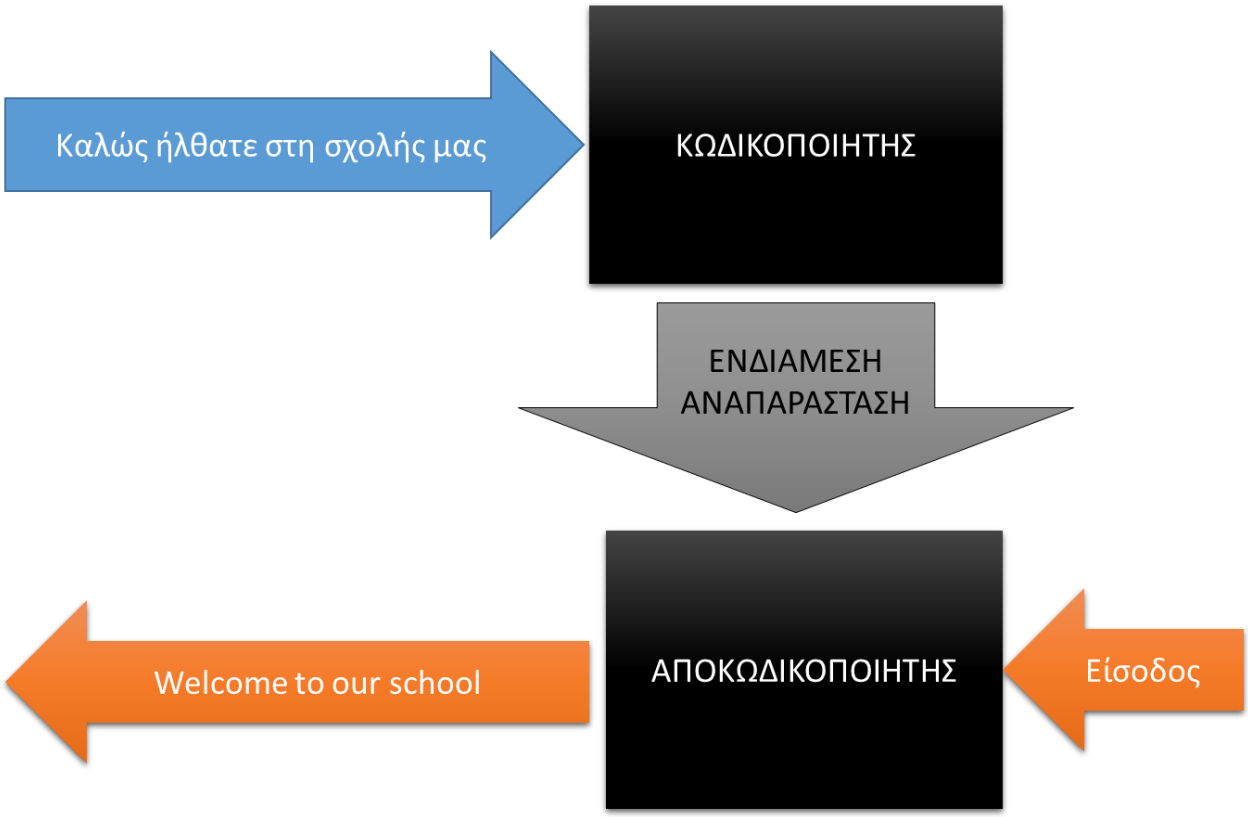
Εικόνα 1: Γενικός Μηχανισμός Auto-Attention

[1] Ο μηχανισμός αυτοπροσοχής – περιγράφεται παρακάτω - μπορεί να υπολογιστεί παράλληλα για όλες τις λέξεις σε μια ακολουθία.

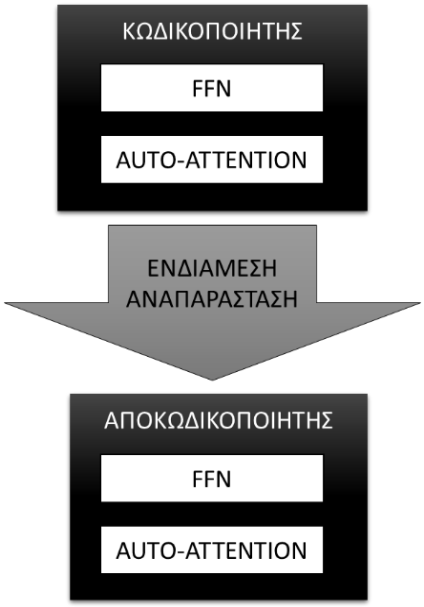
Κάθε Μετασχηματιστής αποτελείται από δύο τμήματα: έναν κωδικοποιητή που επεξεργάζεται την ακολουθία εισόδου και έναν αποκωδικοποιητή, που με βάση την ακολουθία εξόδου η οποία διαμορφώνεται, προβλέπει τα στοιχεία της, κατά τη διάρκεια της εκπαίδευσης [9].

Για παράδειγμα, σε ένα σύστημα αυτόματης μετάφρασης, ο μετασχηματιστής μπορεί να χρησιμοποιεί μια σειρά από λέξεις μίας γλώσσας και να δημιουργεί διαδοχικά την επόμενη αντίστοιχη λέξη της άλλης γλώσσας, μέχρι να μεταφραστεί ολόκληρη η πρόταση.

Τόσο ο κωδικοποιητής, όσο και ο αποκωδικοποιητής, αποτελούνται από πολλαπλά επίπεδα αυτο-προσοχής (self-attention) και νευρωνικών δικτύων ανάδρασης (feed forward neural networks).



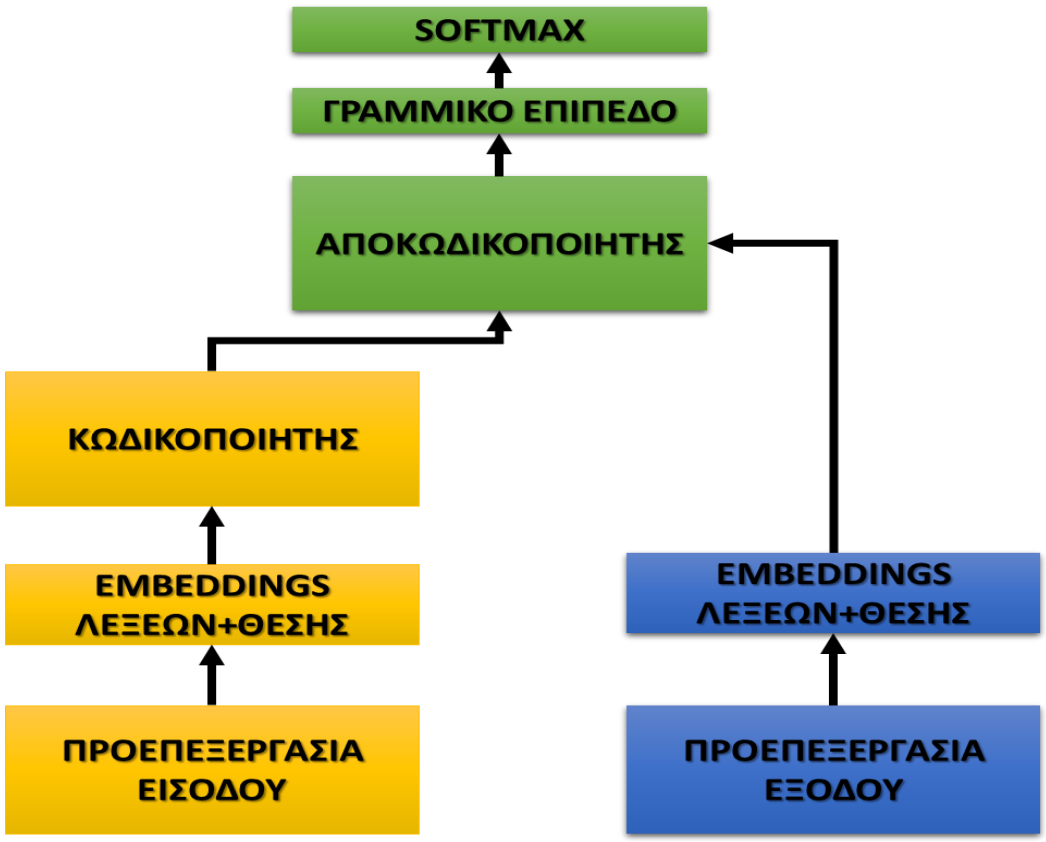
Εικόνα 2: Μετασχηματιστής σε εργασία αυτόματης μετάφρασης



Εικόνα 3: Γενική δομή κωδικοποιητή και αποκωδικοποιητή

Ο κωδικοποιητής λαμβάνει την πρόταση εισόδου και παράγει μια διανυσματική αναπαράσταση σταθερού μεγέθους, η οποία στη συνέχεια τροφοδοτείται στον αποκωδικοποιητή για να δημιουργήσει την πρόταση εξόδου. Ο αποκωδικοποιητής χρησιμοποιεί τόσο την αυτό-προσοχή όσο και την διασταυρούμενη προσοχή (cross attention). Ο μηχανισμός προσοχής εφαρμόζεται στην έξοδο του κωδικοποιητή και στην είσοδο του αποκωδικοποιητή. Ο κωδικοποιητής λαμβάνει μια ακολουθία γλωσσικών στοιχείων και παράγει μια διανυσματική αναπαράσταση σταθερού μεγέθους ολόκληρης της ακολουθίας, η οποία μπορεί στη συνέχεια να χρησιμοποιηθεί για ταξινόμηση (classification). Εφαρμόζει μηχανισμό αυτό-προσοχής στην είσοδο, επιτρέποντάς του να εστιάσει στα πιο σχετικά μέρη της εισόδου για τη δεδομένη εργασία [10].

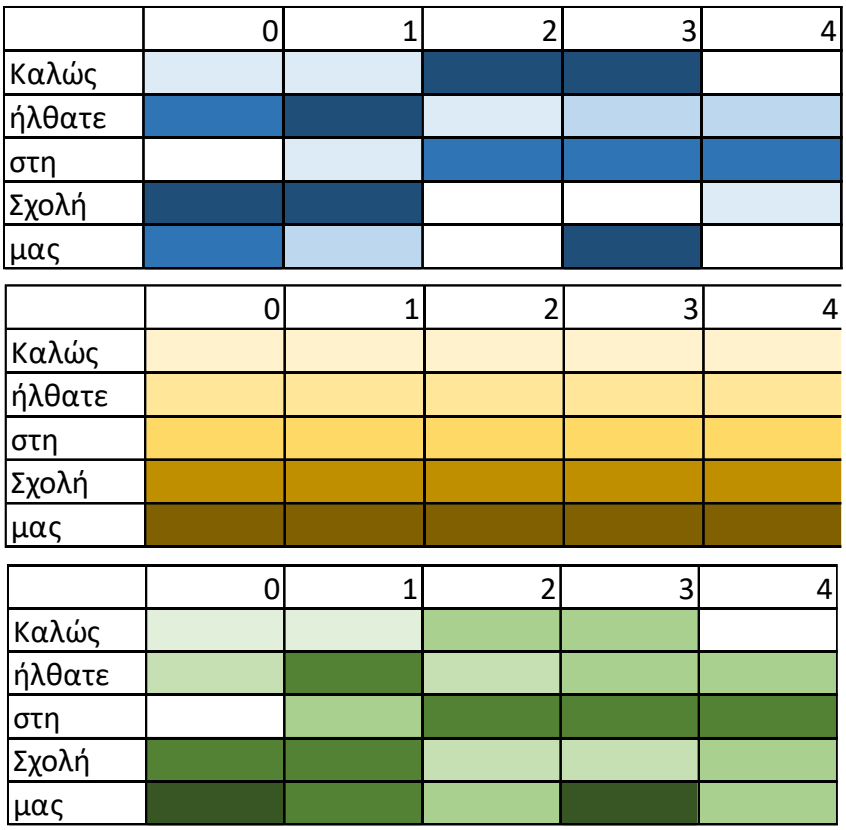
Η γενική λειτουργία των μετασχηματιστών, φαίνεται στο παρακάτω σχήμα:



Εικόνα 4:Γενική Λειτουργία των Μετασχηματιστών

Το γεγονός ότι οι Transformers λαμβάνουν το σύνολο των embeddings[2], επιταχύνει την επεξεργασία τους. Ωστόσο τα embeddings των λέξεων (word embeddings) δεν περιλαμβάνουν πληροφορία σχετικά με τις θέσεις των λέξεων. Το ζήτημα αυτό λύνεται με την προσθήκη των embeddings θέσης (position embeddings). Κάθε στοιχείο (token) του κειμένου, εκτός από το word embedding, διαθέτει και ένα position embedding, το οποίο αντιστοιχεί στη θέση του στην πρόταση. Αυτά συνδυάζονται για να δώσουν την πλήρη αναπαράσταση του. Για την αναπαράσταση των positional embeddings προτάθηκαν κωδικοποιήσεις με χρήση ημιτονοειδών και συνημιτονοειδών συναρτήσεων διαφορετικών συχνοτήτων, χρήση διαφορετικού διανύσματος για κάθε πιθανή θέση της λέξης ή κωδικοποίηση των σχετικών θέσεων των λέξεων. Σε κάθε περίπτωση, τα συνδυαστικά embeddings (δηλαδή τα word embeddings που περιγράφουν τη σημασία της λέξης και τα positional embeddings που περιγράφουν τη θέση της στη φράση) περνούν στην είσοδο του μηχανισμού Self-Attention [11].

Στην παρακάτω εικόνα, φαίνεται σχηματικά η αναπαράσταση του word embedding (μπλε αποχρώσεις) και του position embedding (κίτρινες αποχρώσεις), για τη φράση «Καλώς ήλθατε στη Σχολή μας». Από το συνδυασμό τους προκύπτει η αναπαράσταση που εισέρχεται στον Μετασχηματιστή (πράσινες αποχρώσεις).



Εικόνα 5: Συνδυασμός word και position embedding για τη δημιουργία του embedding που θα αποτελέσει την είσοδο του Transformer

[2] Μορφή διανυσματικών αναπαραστάσεων των λέξεων

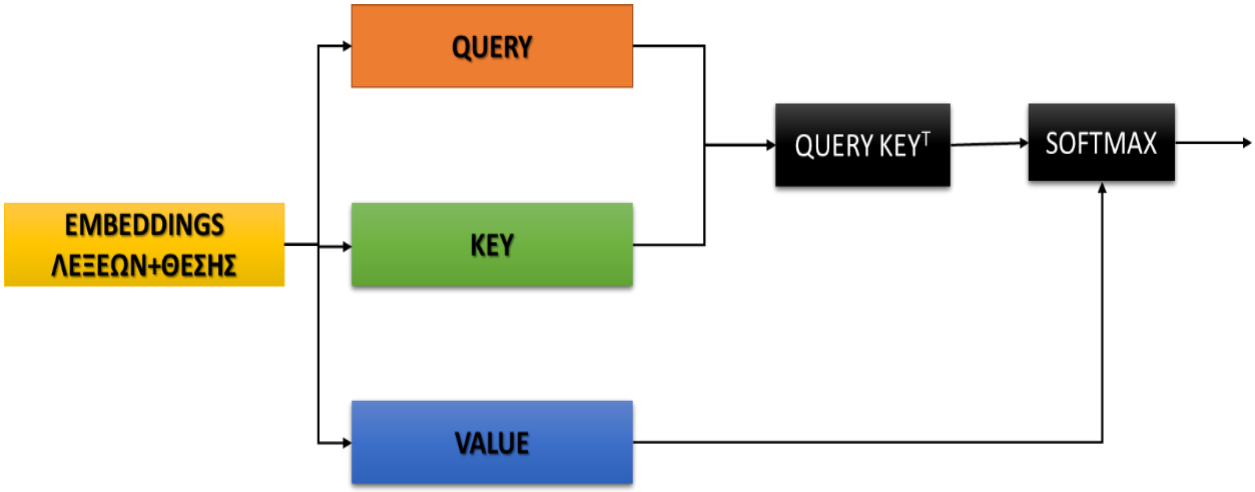
Εκεί, από το ίδιο διάνυσμα εισόδου (το embedding) δημιουργούνται τρεις διαφορετικές προβολές μέσω τριών γραμμικών επιπέδων:

- **Query (Q):** Αντιπροσωπεύει το βαθμό κατά τον οποίο σχετίζεται μία λέξη με τις υπόλοιπες.
- **Key (K):** Αντιπροσωπεύει την πληροφορία που θα χρησιμοποιηθεί για να αξιολογηθεί ο βαθμός προσοχής που θα πρέπει να δοθεί στη λέξη.
- **Value (V):** Αντιπροσωπεύει την πραγματική πληροφορία της λέξης που θα μεταφερθεί και εξαρτάται από το βαθμό συσχέτισης με τις υπόλοιπες λέξεις.

Στη συνέχεια υπολογίζεται το γινόμενο QK^T, που αποτυπώνει το βαθμό με τον οποίο κάθε λέξη συσχετίζεται με τις υπόλοιπες. Το επόμενο βήμα είναι να κανονικοποιηθούν τα αποτελέσματα και να περάσουν από τη συνάρτηση softmax, η οποία τα μετατρέπει σε βάρη στο διάστημα [0,1][3]. Αυτά τα βάρη εφαρμόζονται πάνω στα Values (V), ώστε κάθε λέξη να αναμειχθεί με τις πληροφορίες των άλλων λέξεων ανάλογα με τη σημασία τους [7].

$$Attention(Q,K,V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

Το αποτέλεσμα της διαδικασίας είναι ένας νέος συνδυασμός embeddings: τα αρχικά embeddings εμπλουτισμένα με πληροφορία από όλο το υπόλοιπο πλαίσιο της πρότασης. Αυτό αποτελεί την είσοδο στο επόμενο επίπεδο του Transformer.



[3] Το άθροισμα των βαρών είναι 1. d_k είναι το μέγεθος του παραγομένου διανύσματος

Στο παραπάνω παράδειγμα, κάθε λέξη αντιπροσωπεύεται από ένα διάνυσμά που προέκυψε από το συνδυασμό των embeddings λέξης και θέσης. Αν αναζητείται η συσχέτιση της λέξης «Σχολή» με τις υπόλοιπες, εξετάζεται το εσωτερικό γινόμενο του Q(«Σχολή»)K(«μας»). Αν αυτό προκύψει ότι είναι υψηλό, σημαίνει ότι υπάρχει ισχυρή συσχέτιση μεταξύ των λέξεων «Σχολή» και «μας». Αυτό επαναλαμβάνεται για όλες τις υπόλοιπες λέξεις.

Εφαρμόζεται η συνάρτηση softmax και έστω ότι προκύπτουν οι εξής πιθανότητες ισχυρής συσχέτισης για κάθε λέξη:

- **«μας»:** 0.65
- **«στη»:** 0.20
- **«ήλθατε»:** 0.10
- **«Καλώς»:** 0.05

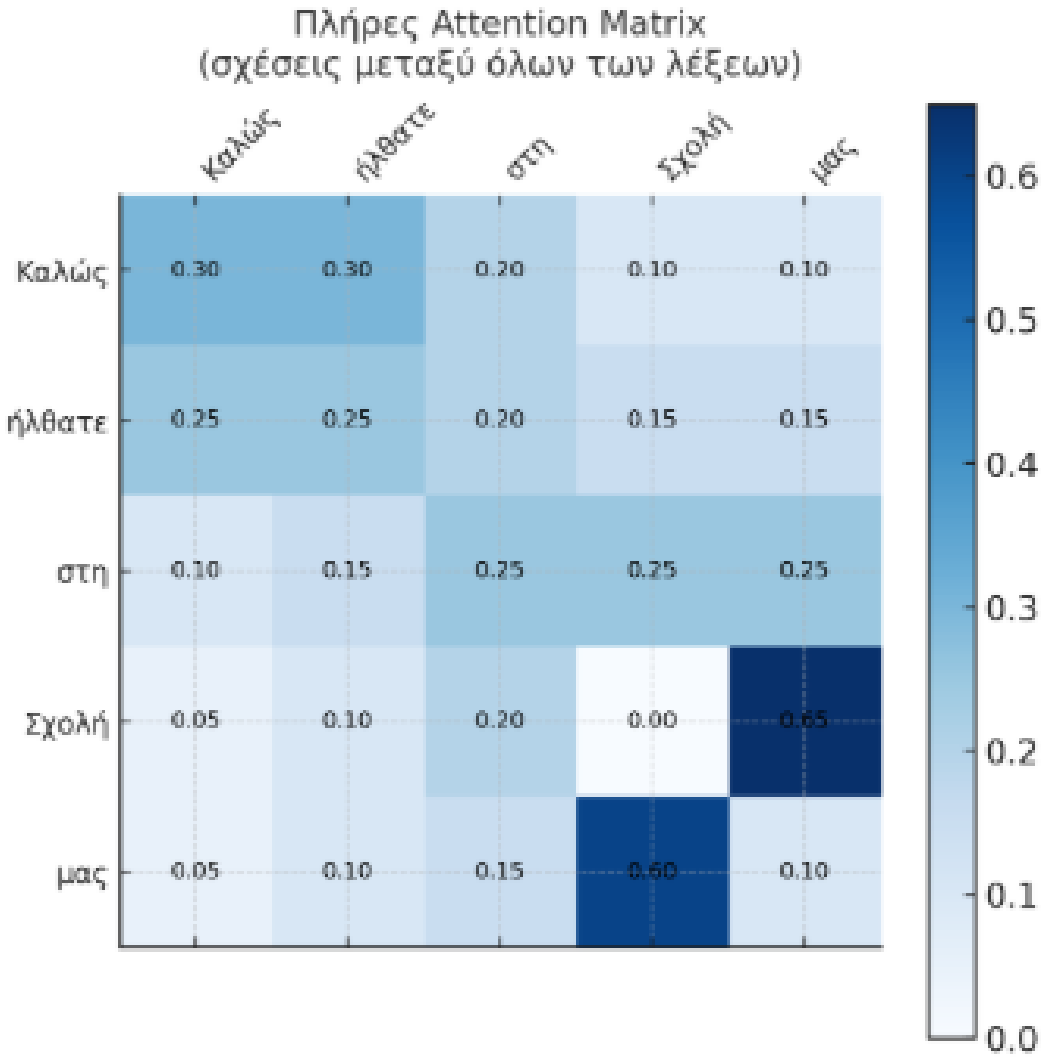
Τα βάρη αυτά εφαρμόζονται στα διανύσματα V ως εξής:

Embedding (Σχολή) **=** 0.65·V(μας)**+**0.20·V(στη)**+**0.10V(ήλθατε)**+**0.05V(Καλώς)

Ο Μετασχηματιστής με αυτό τον τρόπο καταλαβαίνει ότι οι λέξεις «Σχολή» και «μας» συσχετίζονται ισχυρά, ενώ οι λέξεις «Καλώς ήλθατε» είναι ένα ξεχωριστό τμήμα (χαιρετισμός). Αυτό επιτρέπει στο μοντέλο να μεταφράσει σωστά σε «Welcome to our school» και όχι π.χ. "Welcome to the School".

Το αποτέλεσμα της διαδικασίας μέχρι το σημείο αυτό (η έξοδος του Κωδικοποιητή), μπορεί να χρησιμοποιηθεί για την αποδοτική κατηγοριοποίηση κειμένου.

Η παρακάτω εικόνα δείχνει τη συσχέτιση μεταξύ όλων των ζευγών λέξεων της πρότασης.



Εικόνα 6: Πλήρης πίνακας Attention για την πρόταση

Σε ότι αφορά την αξιοποίηση της εξόδου του Κωδικοποιητή για την σύνθεση κειμένου, χρησιμοποιείται η διάταξη του Αποκωδικοποιητή, όπου εξετάζεται κάθε λέξη. Σε κάθε βήμα που εκτελείται στον Αποκωδικοποιητή λαμβάνεται πληροφορία από δύο πηγές [12]:

- **Λέξεις που έχει παραχθεί από τον Αποκωδικοποιητή στα προηγούμενα βήματα (target Self-Attention).**

- **Υπολογισμός τιμών Αυτοπροσοχής με προβολές Q από την ήδη παραχθείσα ακολουθία και K,V από το την είσοδο.**

Στο πρώτο βήμα η έξοδος είναι το ειδικό token <start>. Στη συνέχεια, αφού έχει καταστεί σαφές ότι το «Καλώς ήλθατε» αντιστοιχεί σε χαιρετισμό, παράγει την πρώτη λέξη: «Welcome». Με τη λέξη «Welcome» στο αποτέλεσμα και την πληροφορία της υψηλής συσχέτισης της λέξης «στη» με τη λέξη «Σχολή», εισάγει στο αποτέλεσμα τη λέξη «**to»**.

Στη συνέχεια (και ενώ το αποτέλεσμα είναι ήδη «Welcome to»), αφού από τον κωδικοποιητή υπάρχει η πληροφορία ότι η λέξη «Σχολή» συνδέεται έντονα με τη λέξη «μας», τοποθετείται στο αποτέλεσμα η λέξη «our». Στο σημείο αυτό θα πρέπει να τοποθετηθεί το ουσιαστικό που αντιστοιχεί στη λέξη «our». Αφού από τον κωδικοποιητή προκύπτει ότι οι λέξεις «Σχολή» και «μας», τότε προστίθεται στο αποτέλεσμα η λέξη «School». Επομένως το τελικό αποτέλεσμα είναι η πρόταση «Welcome to our School».

Επίλογος

Οι Μετασχηματιστές μπορούν να χρησιμοποιηθούν σε μία ποικιλία εργασιών, που απαιτείται επεξεργασία φυσικής γλώσσας. Σε εργασίες κατηγοριοποίησης (ανάλυση συναισθήματος, ταξινόμηση κειμένου σε θεματικές κατηγορίες), συνήθως αξιοποιείται αποκλειστικά ο Κωδικοποιητής. Παράδειγμα αποτελούν τα προ-εκπαιδευμένα μοντέλα BERT (Bidirectional Encoder Representations from Transformers)[4]. Όταν απαιτείται η παραγωγή νέας ακολουθίας (sequence-to-sequence), χρησιμοποιείται η πλήρης αρχιτεκτονική Κωδικοποιητή-Αποκωδικοποιητή (αυτόματη μετάφραση, παραγωγή περίληψης κειμένου, σύνθεση απαντήσεων-chatbot).

[4] Δημιουργούν αναπαραστάσεις του κειμένου εισόδου, οι οποίες στη συνέχεια τροφοδοτούνται σε ταξινομητές (classifiers).

Αναφορές.

[1]	Δ. Ντόντος, "Η ικανότητα του μέλλοντος θα προσδιορίζεται πολύ λιγότερο από τους αριθμούς σε προσωπικό και μέσα σε σύγκριση με τις δικτυοκεντρικές εφαρμογές σε τεχνολογίες αυτοματισμούς και κουλτούρα πειραματισμού και καινοτομίας," 2022. [Online]. Available: **https://pandemos.panteion.gr/items/1533c11a-07e1-4edf-bd24-20e56929801c**
[2]	C. Hiramath and G. Deshpande, "Fake News Detection Using Deep Learning Techniques," 2019. [Online]. Available: https://www.researchgate.net/publication/339170194_Fake_News_Detection_Using_Deep_Learning_Techniques.
[3]	D. Jones, "Detecting Propaganda in News Articles Information Systems Seminar Conference," 2023. [Online]. Available: https://www.researchgate.net/publication/376308894_Detecting_Propaganda_in_News_Articles_Information_Systems_Seminar_Conference.
[4]	S. Joseph, H. Hlomani, K. Letsholo, F. Kaniwa and K. Sedimo, "Natural Language Processing: A Review," 2016. [Online]. Available: https://www.icts.res.in/sites/default/files/media/media-library/NLPIntro.pdf.
[5]	R. Keesaram and S. R, "NLP - from Theory to Practice," 2023. [Online]. Available: https://www.prepvector.com/blog/nlp-from-theory-to-practice.
[6]	C. Y. Kesiku, A. Chaves-Villota and B. Garcia-Zapirain, "Natural Language Processing Techniques for Text Classification of Biomedical Documents: A Systematic Review," 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/10/499.
[7]	N. S. N. P. J. U. L. J. A. N. G. L. K. I. P. Ashish Vaswani, "Attention Is All You Need," 2017. [Online]. Available: https://arxiv.org/abs/1706.03762.
[8]	Z. Huang, M. Liang, J. Qin, S. Zhong and L. Lin, "Understanding Self-attention Mechanism via Dynamical System Perspective," 2023. [Online]. Available: https://openaccess.thecvf.com/content/ICCV2023/papers/Huang_Understanding_Self-attention_Mechanism_via_Dynamical_System_Perspective_ICCV_2023_paperpdf.
[9]	F. Yvon, "Transformers in Natural Language Processin," 2023. [Online]. Available: https://hal.science/hal-04224531v1.
[10]	S. Kamatala, A. K. Jonnalagadda and P. Naayini, "Transformers beyond nlp: Expanding horizons in machine learning," 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5112305.

[11]	L. D. V. S. J. C. C. D. M. P. C. T. R. R. L. M. F. J. D. S. P. v. P. C. M. Y. J. J. P. C. X. L. S. S. Thomas Wolf, "Transformers: State-of-the-Art Natural Language Processing," 2020. [Online]. Available: https://aclanthology.org/2020.emnlp-demos.6.pdf.
[12]	U. Kamath, K. Graham and W. Emara, Transformers for machine learning, Boca Raton: CRC, 2022.

Βιογραφικό συντάκτη.

Ο Σχης (ΠΛΗ) Δημήτριος Ντόντος αποφοίτησε από τη Στρατιωτική Σχολή Ευελπίδων (ΣΣΕ) το 1996 ως Ανθλγός (ΠΖ). Το 2002 αποφοίτησε από τη ΣΠΗΥ και το 2007 μετατάχθηκε στο Σώμα Έρευνας Πληροφορικής. Είναι απόφοιτος της Ανώτατης Διακλαδικής Σχολής Πολέμου (2013) και της Σχολής Εθνικής Αμύνης (2021). Κατέχει Μεταπτυχιακό Δίπλωμα στις Νέες Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών (ΕΚΠΑ) και Διεθνείς Σπουδές Ασφάλειας (Πάντειο Πανεπιστήμιο). Είναι υποψήφιος διδάκτορας του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Ιωαννίνων με αντικείμενο διατριβής: «ανάλυση δεδομένων κυβερνοασφάλειας με μεθόδους μηχανικής μάθησης».

Dark Web:
(Χαρακτηριστικά - Αρχιτεκτονικές – Πρωτόκολλα εφαρμογές)
Εξέλιξη του Πολέμου: Η Τεχνολογία των UAVs στις Σύγχρονες Στρατιωτικές Επιχειρήσεις

Υπολοχαγός (ΔΒ) Θεόδωρος Ραϊόπουλος

Εισαγωγή

Το Dark Web είναι ένα μέρος του διαδικτύου που δεν είναι προσβάσιμο μέσω των συνηθισμένων μηχανών αναζήτησης όπως το Google και απαιτεί ειδικό λογισμικό, όπως το Tor (The Onion Router), για την πρόσβαση. Αποτελεί μέρος του Deep Web, το οποίο περιλαμβάνει περιεχόμενο που δεν είναι ευρετηριασμένο από τις μηχανές αναζήτησης, όπως ιδιωτικά αρχεία, βάσεις δεδομένων και εσωτερικά δίκτυα. Το Dark Web χρησιμοποιείται για ανώνυμη επικοινωνία και συναλλαγές, καθώς παρέχει υψηλό επίπεδο ανωνυμίας στους χρήστες. Χρησιμοποιείται για νόμιμες δραστηριότητες, όπως η προστασία της ιδιωτικότητας και η αποφυγή κυβερνητικής λογοκρισίας, αλλά και για παράνομες δραστηριότητες, όπως η διακίνηση ναρκωτικών, η πώληση όπλων και η κυβερνοεγκληματικότητα. Παρόλο που το Dark Web έχει αποκτήσει κακή φήμη, αποτελεί επίσης εργαλείο για δημοσιογράφους, ακτιβιστές και χρήστες που επιδιώκουν την προστασία της ιδιωτικής τους ζωής.

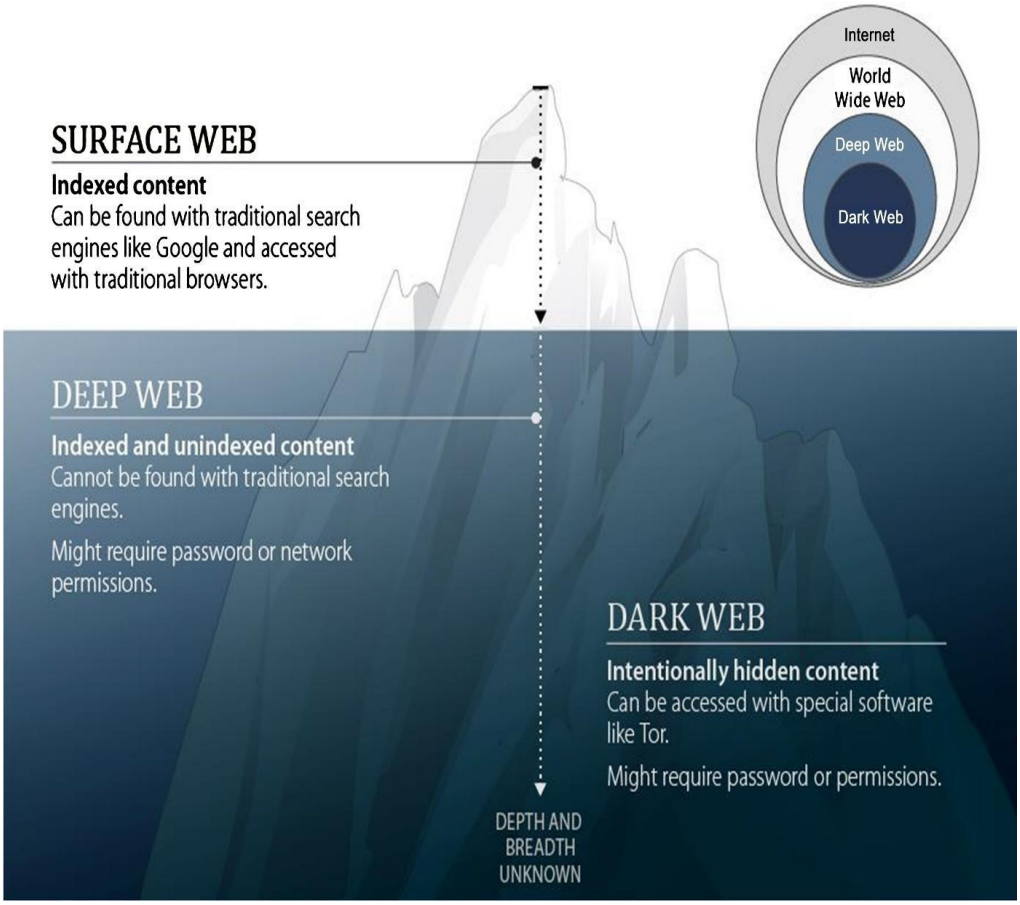
Διαχωρισμός μεταξύ Surface Web, Deep Web και Dark Web

Το διαδίκτυο χωρίζεται σε τρεις βασικές κατηγορίες: Surface Web, Deep Web και Dark Web. Το Surface Web είναι το κομμάτι του διαδικτύου που είναι προσβάσιμο από οποιονδήποτε μέσω των συνηθισμένων μηχανών αναζήτησης, όπως το Google ή το Bing. Περιλαμβάνει ιστοσελίδες ειδήσεων, μέσα κοινωνικής δικτύωσης, ηλεκτρονικά καταστήματα και οποιοδήποτε άλλο περιεχόμενο που μπορεί να αναζητηθεί και να εμφανιστεί στα αποτελέσματα αναζήτησης. Παράδειγμα: ιστοσελίδες όπως Wikipedia, Facebook, YouTube.

Το Deep Web αποτελεί το μεγαλύτερο μέρος του διαδικτύου και περιλαμβάνει περιεχόμενο που δεν είναι ευρετηριασμένο από τις μηχανές αναζήτησης. Πρόκειται για ιδιωτικά δεδομένα, όπως τραπεζικοί λογαριασμοί, email, ιατρικά αρχεία και βάσεις δεδομένων εταιρειών. Αυτές οι πληροφορίες απαιτούν εξουσιοδότηση ή ειδική πρόσβαση. Παράδειγμα: Gmail inbox, online τραπεζικές υπηρεσίες, εταιρικά intranet.

Το Dark Web είναι ένα μικρό μέρος του Deep Web που απαιτεί εξειδικευμένο λογισμικό, όπως το Tor, για την πρόσβαση.

Χρησιμοποιείται για ανώνυμη επικοινωνία και συναλλαγές, αλλά και για παράνομες δραστηριότητες, όπως διακίνηση ναρκωτικών και hacking. Ωστόσο, χρησιμοποιείται επίσης από ακτιβιστές και δημοσιογράφους σε χώρες με λογοκρισία. Παράδειγμα: αγορές όπως το Silk Road (πλέον κλειστό), φόρουμ ανωνύμων ακτιβιστών (Εικόνα 1).



Εικόνα 1. Αναπαράσταση Surface Web, Deep Web, Dark Web.

Βασικά Χαρακτηριστικά του Dark Web

Ανωνυμία και κρυπτογράφηση

Η ανωνυμία και η κρυπτογράφηση αποτελούν θεμελιώδη χαρακτηριστικά του Dark Web, επιτρέποντας στους χρήστες να παραμένουν ανώνυμοι και να προστατεύουν τα δεδομένα τους από παρακολούθηση.

Το πιο διαδεδομένο δίκτυο ανωνυμίας, το Tor (The Onion Router), χρησιμοποιεί ένα σύστημα πολυεπίπεδης κρυπτογράφησης, γνωστό ως onion routing, όπου η διαδικτυακή κίνηση περνάει μέσα από πολλαπλούς κόμβους, καθιστώντας δύσκολο τον εντοπισμό της αρχικής διεύθυνσης IP. Παρόμοια, το I2P (Invisible Internet Project) χρησιμοποιεί garlic routing, κρυπτογραφώντας πολλαπλά μηνύματα μαζί, ώστε να αυξάνει την ασφάλεια και την ιδιωτικότητα. Αυτές οι τεχνολογίες χρησιμοποιούνται όχι μόνο για νόμιμους σκοπούς, όπως η προστασία πληροφοριοδοτών και ακτιβιστών, αλλά και για παράνομες δραστηριότητες, όπως το cybercrime και το εμπόριο παράνομων αγαθών. Η κρυπτογράφηση, μέσω πρωτοκόλλων όπως το PGP (Pretty Good Privacy), εξασφαλίζει ασφαλή επικοινωνία, ενισχύοντας τόσο την ελευθερία της έκφρασης όσο και την εγκληματική δραστηριότητα στο Dark Web.

Δομή και προσβασιμότητα

Η δομή του βασίζεται σε ένα πολυεπίπεδο σύστημα ανωνυμίας, όπου η πρόσβαση γίνεται μέσω εξειδικευμένων προγραμμάτων περιήγησης, όπως το Tor (The Onion Router). Το Dark Web χωρίζεται σε διαφορετικά επίπεδα (στρώματα), με το επιφανειακό επίπεδο να περιλαμβάνει ιστοσελίδες που είναι σχετικά εύκολες στην πρόσβαση, ενώ τα βαθύτερα επίπεδα απαιτούν ειδικά κλειδιά ή προσκλήσεις. Για παράδειγμα, το Hidden Wiki λειτουργεί ως κατάλογος για διάφορες σελίδες του Dark Web, ενώ πιο κρυφές υπηρεσίες, όπως αγορές του Silk Road (πριν το κλείσιμό του), απαιτούσαν πρόσθετη επαλήθευση. Η προσβασιμότητα στο Dark Web είναι περιορισμένη, καθώς οι διευθύνσεις των ιστότοπων είναι μορφής .onion, καθιστώντας τες δυσανάγνωστες και δυναμικά μεταβαλλόμενες για επιπλέον προστασία.

Νομιμότητα και ηθικά ζητήματα

Η νομιμότητα του Dark Web είναι ένα αμφιλεγόμενο ζήτημα, καθώς η χρήση του από μόνη της δεν είναι παράνομη, αλλά το περιεχόμενό του συχνά περιλαμβάνει δραστηριότητες που παραβιάζουν τον νόμο. Πολλές κυβερνήσεις αναγνωρίζουν τη σημασία του για την προστασία των ανθρωπίνων δικαιωμάτων, καθώς επιτρέπει σε δημοσιογράφους και ακτιβιστές να επικοινωνούν ανώνυμα σε καταπιεστικά καθεστώτα. Ωστόσο, η έλλειψη ελέγχου έχει οδηγήσει στη διάδοση παράνομου εμπορίου, παιδικής εκμετάλλευσης και κυβερνοεγκλήματος, δημιουργώντας νομικά και ηθικά διλήμματα. Για την αντιμετώπιση αυτών των προβλημάτων, έχουν θεσπιστεί νόμοι και διεθνείς πρωτοβουλίες. Το FOSTA (Fight Online Sex Trafficking Act – SESTA (Stop Enabling Sex Traffickers Act) Act (2018) στις ΗΠΑ επιχειρεί να περιορίσει την εκμετάλλευση μέσω διαδικτυακών πλατφορμών, ενώ η Ευρωπαϊκή Ένωση, με τον Κανονισμό για τις Ψηφιακές Υπηρεσίες (Digital Services Act, 2022), επιβάλλει αυστηρότερους ελέγχους στο παράνομο περιεχόμενο. Επιπλέον, διεθνή συνέδρια, όπως το INTERPOL World και το United Nations Internet Governance Forum (IGF), συζητούν τρόπους για τη ρύθμιση του Dark Web χωρίς να υπονομεύσουν τη διαδικτυακή ιδιωτικότητα.

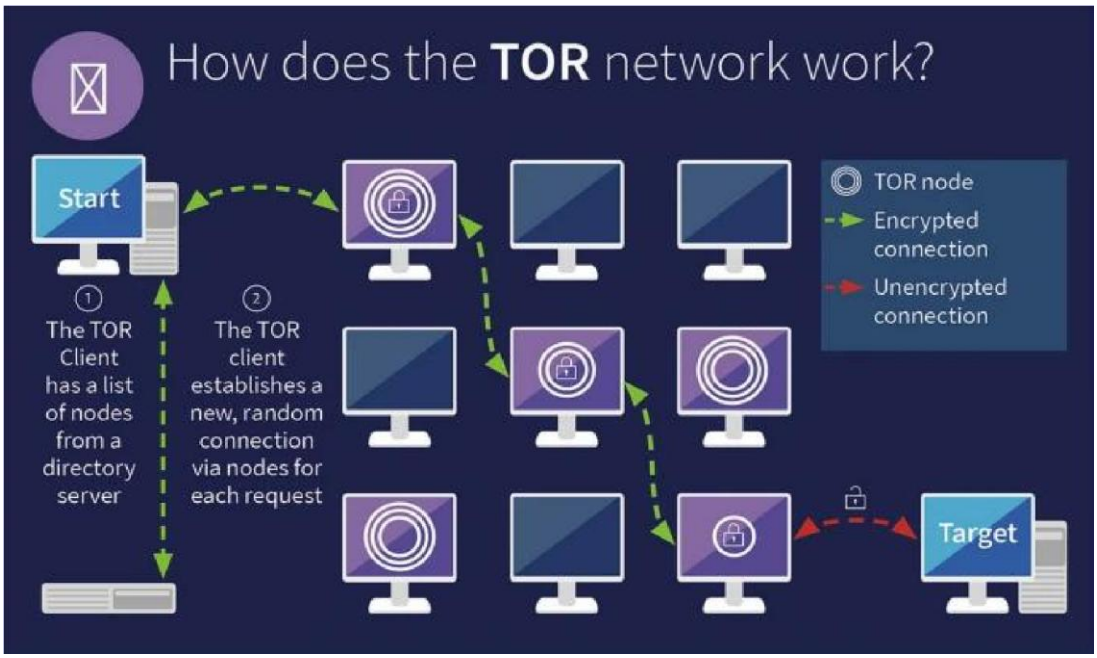
Ωστόσο, η αποκεντρωμένη και ανώνυμη φύση της τεχνολογίας καθιστά δύσκολη την πλήρη εξάλειψη της παρανομίας, με αποτέλεσμα το Dark Web να παραμένει ένα πεδίο έντονης νομικής και ηθικής αντιπαράθεσης.

Αρχιτεκτονικές και Πρωτόκολλα

Δίκτυα ανωνυμίας (Tor, I2P, Freenet)

Τα δίκτυα ανωνυμίας αποτελούν βασικούς μηχανισμούς προστασίας της ιδιωτικότητας και της ανωνυμίας στο διαδίκτυο, επιτρέποντας την πρόσβαση σε κρυφές υπηρεσίες και τη μεταφορά δεδομένων χωρίς την αποκάλυψη της ταυτότητας του χρήστη. Τα τρία πιο διαδεδομένα δίκτυα ανωνυμίας είναι το Tor (The Onion Router), το I2P (Invisible Internet Project) και το Freenet, καθένα με διαφορετικές αρχές λειτουργίας και χρήσεις.

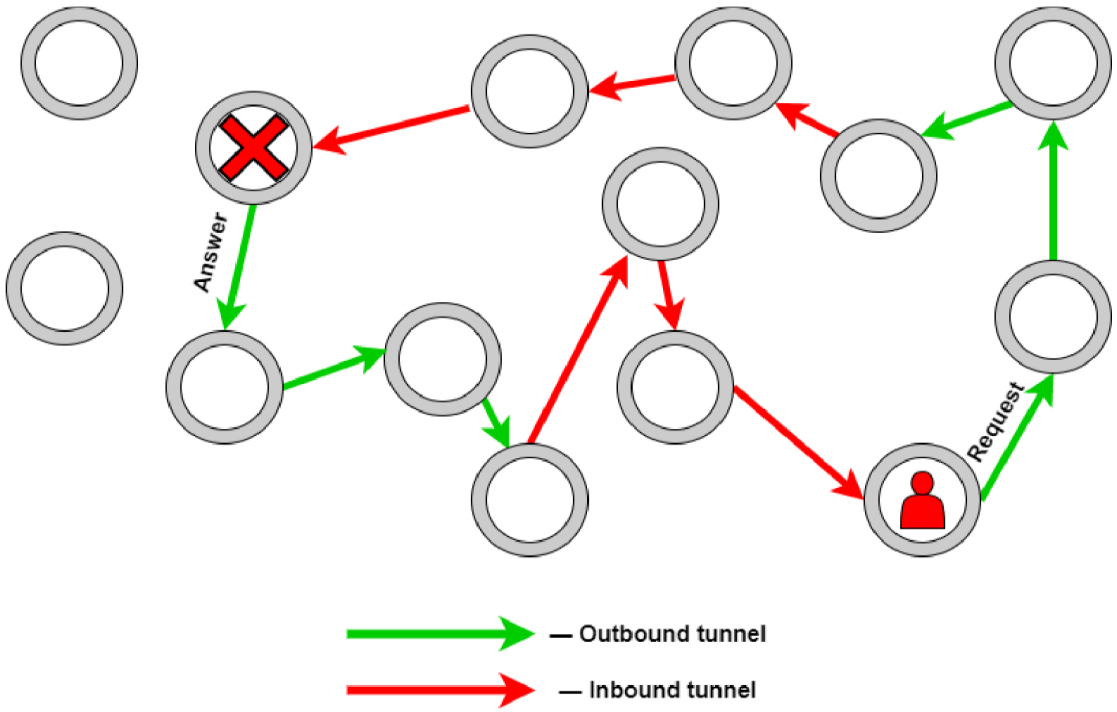
Το Tor είναι το πιο γνωστό δίκτυο ανωνυμίας, χρησιμοποιώντας την τεχνική του onion routing. Το Tor (The Onion Router) αναπτύχθηκε το 2002 από το Ναυτικό των ΗΠΑ και αργότερα έγινε δημόσια διαθέσιμο ως εργαλείο ανώνυμης περιήγησης. Χρησιμοποιεί onion routing, όπου κάθε πακέτο δεδομένων διέρχεται από τυχαίους κόμβους (nodes) (βλέπε Εικόνα 2) με διαδοχική κρυπτογράφηση σε κάθε επίπεδο, ώστε κανένας κόμβος να μην γνωρίζει πλήρως την προέλευση και τον προορισμό. Το Tor είναι ιδανικό για πρόσβαση σε .onion ιστότοπους, όπως ανώνυμα forums, ανεξάρτητα μέσα ενημέρωσης (ProPublica), καθώς και μηχανές αναζήτησης που δεν καταγράφουν δεδομένα (DuckDuckGo).



Εικόνα 2. Λειτουργία του TOR network.

Το I2P (Invisible Internet Project) εμφανίστηκε το 2003 και διαφέρει από το Tor, καθώς είναι σχεδιασμένο για ανώνυμη επικοινωνία μεταξύ χρηστών (peer-to-peer) και όχι για περιήγηση στο διαδίκτυο. Χρησιμοποιεί garlic routing, όπου πολλά πακέτα δεδομένων κρυπτογραφούνται μαζί για να αποτρέψουν την ανίχνευση της επικοινωνίας. Όλα τα αιτήματα κρυπτογραφούνται στην πλευρά του αποστολέα και αποκρυπτογραφούνται στην πλευρά του παραλήπτη χρησιμοποιώντας τους αλγόριθμους NTCP2 (NIO Transmission Control Protocol v2) και SSU (Secure Semireliable UDP), που είναι τα κρυπτογραφικά αντίστοιχα των TCP και UDP στο I2P. Αυτοί οι αλγόριθμοι εξασφαλίζουν ότι κανείς, ούτε οι ενδιάμεσοι κόμβοι ούτε οι μηχανές αναζήτησης, δεν μπορούν να παρακολουθήσουν τα αιτήματα.

Το I2P αποτελείται από routers, endpoints και tunnels. Οι routers συνδέονται με κανονικές και I2P διευθύνσεις και μεταφέρουν αιτήματα μέσω tunnels που αποτελούνται από διάφορους κόμβους. Ο χρήστης καθορίζει τον προορισμό και το μήκος του tunnel, εξασφαλίζοντας πλήρη ανωνυμία. Αυτό μπορεί να απεικονιστεί με ένα παράδειγμα: Ένα φορτηγό (το αίτημα) διασχίζει πολλές οδούς (τους κόμβους του tunnel) χωρίς να σταματά σε κανέναν σταθμό ελέγχου (ενδιάμεσους κόμβους), οπότε κανείς δεν γνωρίζει που πηγαίνει ή τι μεταφέρει. Μόνο ο τελικός προορισμός μπορεί να το σταματήσει, εξασφαλίζοντας την ανωνυμία του αιτήματος (βλέπε Εικόνα 3). Το I2P είναι ιδανικό για ανώνυμες συνομιλίες, ανταλλαγή αρχείων και ανώνυμα blogs.



Εικόνα 3. Παράδειγμα απεικόνισης λειτουργίας I2P (Invisible Internet Project).

Το Freenet ιδρύθηκε πρώτο, το 2000, από τον Ian Clarke, ως ένα αποκεντρωμένο δίκτυο αποθήκευσης δεδομένων. Δεν λειτουργεί όπως ένα κλασικό διαδίκτυο περιήγησης, αλλά ως αποθετήριο δεδομένων, όπου οι χρήστες διαμοιράζονται και αποθηκεύουν κρυπτογραφημένα αρχεία. Οι πληροφορίες διανέμονται μεταξύ πολλών υπολογιστών χωρίς συγκεκριμένους κεντρικούς διακομιστές, κάνοντας δύσκολο τον εντοπισμό της πηγής. Χρησιμοποιείται κυρίως για ανώνυμα blogs, εναλλακτικά ειδησεογραφικά δίκτυα και διατήρηση λογοκριμένου περιεχομένου. Παρότι και τα τρία δίκτυα εξασφαλίζουν ανωνυμία, το Tor είναι το πιο διαδεδομένο για ανώνυμη περιήγηση, το I2P για peer-to-peer επικοινωνία, ενώ το Freenet ειδικεύεται στην αποθήκευση δεδομένων με ανωνυμία.

Μέθοδοι προστασίας προσωπικών δεδομένων στο Dark web

Στο Dark Web, οι χρήστες εφαρμόζουν διάφορες μεθόδους για την προστασία των προσωπικών τους δεδομένων και της ανωνυμίας τους. Οι βασικές μέθοδοι περιλαμβάνουν:

1. Τα δίκτυα ανωνυμίας Tor και I2P που προαναφέρθηκαν.
2. Χρησιμοποίηση ισχυρών μεθόδων κρυπτογράφησης, όπως το AES και το RSA, για να προστατεύσουν τα δεδομένα κατά τη μεταφορά τους.
3. Αποφυγή χρήσης προσωπικών πληροφοριών. Χρησιμοποιούν ψευδώνυμα ή ανώνυμες ταυτότητες για να προστατεύσουν την προσωπικότητά τους. Σε φόρουμ του Dark Web, ένας χρήστης μπορεί να δημιουργήσει λογαριασμό με όνομα "User1234" χωρίς να χρησιμοποιεί το πραγματικό του όνομα ή άλλες προσωπικές πληροφορίες.
4. Πραγματοποίηση συναλλαγών μέσω κρυπτονομισμάτων. Τα κρυπτονομίσματα όπως το Bitcoin και το Monero είναι δημοφιλή στο Dark Web. Ειδικά το Monero, λόγω της ενισχυμένης ανωνυμίας του, επιτρέπει ασφαλείς συναλλαγές χωρίς να αποκαλύπτει τα στοιχεία των χρηστών.
5. Οι χρήστες του Dark Web αντιμετωπίζουν αυξημένους κινδύνους από ιούς και κακόβουλο λογισμικό. Για την προστασία τους, χρησιμοποιούν ισχυρά antivirus και firewalls. Επίσης, συνδέονται συχνά μέσω VPN για να κρύψουν τη διεύθυνση IP τους.

Εφαρμογές του Dark Web

Θετικές χρήσεις

Ιδιωτικότητα

Το Dark Web προσφέρει ανωνυμία σε χρήστες που θέλουν να προστατεύσουν τα προσωπικά τους δεδομένα από εταιρείες, κυβερνήσεις ή χάκερς.

Ένας ακτιβιστής χρησιμοποιεί το Tor για να επικοινωνήσει ανώνυμα χωρίς να παρακολουθείται από κρατικούς φορείς.

Ελευθερία του Λόγου

Σε χώρες με λογοκρισία, το Dark Web επιτρέπει στους πολίτες να εκφραστούν ελεύθερα χωρίς φόβο καταστολής. Δημοσιογράφοι στην Κίνα χρησιμοποιούν το I2P για να δημοσιεύουν ειδήσεις που απαγορεύονται στο κανονικό διαδίκτυο.

Προστασία Πληροφοριοδοτών

Το Dark Web επιτρέπει σε πληροφοριοδότες να αποκαλύπτουν σκάνδαλα χωρίς να αποκαλύπτεται η ταυτότητά τους. Ο ιστότοπος SecureDrop επιτρέπει στους whistleblowers να στέλνουν ανώνυμα έγγραφα σε δημοσιογράφους.

Έρευνα & Δημοσιογραφία

Δημοσιογράφοι και ερευνητές χρησιμοποιούν το Dark Web για να συλλέξουν πληροφορίες και να επικοινωνήσουν με πηγές με ασφάλεια. Ρεπόρτερ του BBC χρησιμοποιεί το Tor για να μιλήσει με πηγές από χώρες με αυστηρή λογοκρισία.

Πρόσβαση σε Πληροφορίες

Το Dark Web επιτρέπει σε ανθρώπους από χώρες με αυστηρό έλεγχο του διαδικτύου να αποκτούν πρόσβαση σε πληροφορίες. Πολίτες στο Ιράν χρησιμοποιούν ανώνυμες υπηρεσίες για να διαβάζουν ξένα ειδησεογραφικά πρακτορεία.

Ασφαλής Επικοινωνία

Παρέχει ασφαλή πλατφόρμες επικοινωνίας, όπως κρυπτογραφημένες συνομιλίες. Ακτιβιστές χρησιμοποιούν Encrypted Email Services για να αποφύγουν την παρακολούθηση.

Εκπαίδευση & Μάθηση

Προσφέρει πρόσβαση σε εκπαιδευτικό υλικό για χρήστες σε χώρες όπου το διαδίκτυο είναι περιορισμένο. Μαθητές στη Βόρεια Κορέα χρησιμοποιούν το Dark Web για να αποκτήσουν πρόσβαση σε διεθνή ακαδημαϊκά άρθρα.

Προστασία από την Παρακολούθηση

Βοηθά χρήστες να αποφύγουν κυβερνητική ή εταιρική παρακολούθηση. Πολίτες σε καταπιεστικά καθεστώτα χρησιμοποιούν VPN και Tor για να αποτρέψουν την ανάλυση της διαδικτυακής τους δραστηριότητας.

Παράκαμψη Γεωγραφικών Περιορισμών

Το Dark Web επιτρέπει την πρόσβαση σε περιεχόμενο που είναι αποκλεισμένο σε ορισμένες περιοχές. Ένας χρήστης από την Τουρκία χρησιμοποιεί Tor για να αποκτήσει πρόσβαση στο Twitter, που είναι λογοκριμένο.

Υπεράσπιση Ψηφιακών Δικαιωμάτων

Οργανώσεις χρησιμοποιούν το Dark Web για την προώθηση των ψηφιακών ελευθεριών και των ανθρωπίνων δικαιωμάτων. Η Electronic Frontier Foundation (EFF) υποστηρίζει εργαλεία που προωθούν την ιδιωτικότητα στο διαδίκτυο.

Παράνομες δραστηριότητες (αγορές ναρκωτικών, όπλων, πλαστών εγγράφων, κυβερνοέγκλημα)

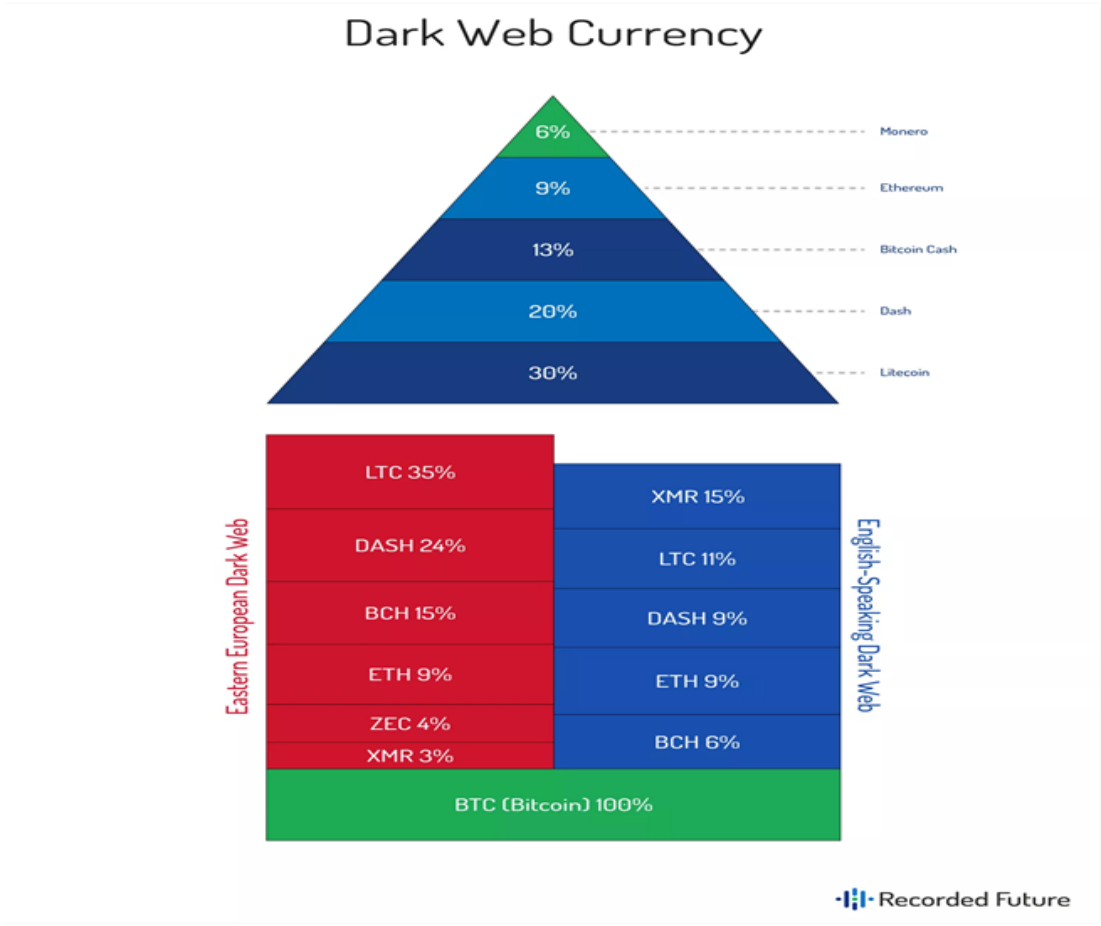
Εικόνα 4. Διάγραμμα απεικόνισης υπηρεσιών Dark Web.

Τα εγκλήματα με μυστικές συναλλαγές – είτε αφορούν ναρκωτικά, χρήματα ή ακόμα και ανθρώπους – διαπράττονται συχνά μέσω του Dark Web (βλέπε Εικόνα 4). Ακολουθούν ορισμένα παραδείγματα εγκληματικών δραστηριοτήτων:

- Δολοφονίες επί πληρωμή: Ιστότοποι όπως το Besa Mafia χρησιμοποιήθηκαν ως αγορές για συμβόλαια θανάτου.
- Εκβιασμός: Σε μία απάτη, οι δράστες απειλούσαν να δημοσιοποιήσουν ευαίσθητες πληροφορίες ή προσωπικές φωτογραφίες, εκτός αν το θύμα πλήρωνε ένα συγκεκριμένο ποσό σε Bitcoin.
- Παράνομες πωλήσεις ναρκωτικών: Το AlphaBay ήταν η μεγαλύτερη αγορά ναρκωτικών στο Dark Web, όπου διακινούνταν φαιντανύλη και ηρωίνη, μέχρι που το Υπουργείο Δικαιοσύνης των ΗΠΑ το έκλεισε το 2017.

- Παράνομες πωλήσεις όπλων: Σύμφωνα με εκτιμήσεις, δεκάδες χιλιάδες δολάρια σε όπλα πωλούνται παράνομα κάθε μήνα μέσω του Dark Web.
- Εμπορία ανθρώπων: Το 2015, η Εισαγγελία της Νέας Υόρκης χρησιμοποίησε ένα πειραματικό εργαλείο διαδικτυακής έρευνας για να εντοπίσει και να συλλάβει τον ηγέτη ενός κυκλώματος εμπορίας ανθρώπων.
- Τρομοκρατία: Ομάδες όπως το Ισλαμικό Κράτος χρησιμοποιούν το Dark Web για στρατολόγηση μελών και σχεδιασμό επιθέσεων.
- Παιδική πορνογραφία: Υπολογίζεται ότι 144.000 Βρετανοί χρήστες είχαν πρόσβαση σε παράνομο περιεχόμενο παιδικής κακοποίησης μέσω του Dark Web το 2018.

Ο ρόλος των κρυπτονομισμάτων στο Dark Web.



Εικόνα 5. Κρυπτονομίσματα στο Dark Web ανά ποσοστό χρήσης.

Τα κρυπτονομίσματα αποτελούν τον κύριο τρόπο συναλλαγών στο Dark Web, καθώς προσφέρουν ανωνυμία, ταχύτητα και δυσκολία εντοπισμού. Η πιο δημοφιλής επιλογή είναι το Bitcoin (BTC), λόγω της μεγάλης αποδοχής του και της ευκολίας στη χρήση. Ωστόσο, επειδή το Bitcoin δεν είναι απολύτως ανώνυμο (όλες οι συναλλαγές καταγράφονται στο blockchain και μπορούν να αναλυθούν), πολλοί χρήστες στρέφονται σε πιο ιδιωτικά νομίσματα, όπως το Monero (XMR) και το Litecoin (LTC) (βλ. Εικόνα 5).

Το Monero (XMR) είναι ιδιαίτερα δημοφιλές επειδή προσφέρει ενισχυμένη ανωνυμία μέσω της τεχνολογίας Ring Signatures και Stealth Addresses, που κρύβουν τον αποστολέα, τον παραλήπτη και το ποσό της συναλλαγής. Το Litecoin (LTC), αν και λιγότερο ανώνυμο από το Monero, χρησιμοποιείται ευρέως λόγω των ταχύτερων συναλλαγών και των χαμηλών προμηθειών του σε σχέση με το Bitcoin.

Τα κρυπτονομίσματα χρησιμοποιούνται στο Dark Web για διάφορες συναλλαγές, όπως αγορά ναρκωτικών, ψεύτικων εγγράφων, όπλων, ransomware πληρωμές και υπηρεσίες hacking. Παράλληλα, χρησιμεύουν και για νόμιμες δραστηριότητες, όπως η χρηματοδότηση ακτιβιστών, η ανώνυμη δωρεά σε δημοσιογράφους ή η αγορά νόμιμων υπηρεσιών φιλοξενίας.

Η ανωνυμία και η μη δυνατότητα αντιστροφής πληρωμών καθιστούν τα κρυπτονομίσματα βασικό εργαλείο για το Dark Web, καθώς οι χρήστες αποφεύγουν τον εντοπισμό από κυβερνήσεις και διωκτικές αρχές.

Μέθοδοι Ανίχνευσης και Αντιμετώπισης

Τεχνικές παρακολούθησης και επιβολής του νόμου

Οι τεχνικές παρακολούθησης και επιβολής του νόμου στο Dark Web περιλαμβάνουν προηγμένες μεθόδους ανάλυσης δεδομένων, επιτήρησης και επιχειρήσεων παγίδευσης (honeypots). Οι αρχές χρησιμοποιούν OSINT (Open Source Intelligence), αναλύοντας δημόσια διαθέσιμες πληροφορίες και συνδέοντας ψευδώνυμα με πραγματικές ταυτότητες μέσω διαρροών δεδομένων. Παράλληλα, αξιοποιούν blockchain analysis για την ιχνηλάτηση παράνομων συναλλαγών σε κρυπτονομίσματα, καθώς πολλές αγοραπωλησίες στο Dark Web γίνονται μέσω Bitcoin ή Monero.

Επιπλέον, ειδικές ομάδες της Europol και του FBI διεισδύουν σε παράνομα φόρουμ και αγορές, προσποιούμενες ότι είναι εγκληματίες για τη συλλογή πληροφοριών και τη σύλληψη υπόπτων. Οι τεχνικές traffic analysis επιτρέπουν την αποκάλυψη κρυμμένων υπηρεσιών του Tor, ενώ ευπάθειες στο λογισμικό ή λάθη των χρηστών μπορούν να αποκαλύψουν τις διευθύνσεις IP τους.

Η συνεργασία διεθνών αρχών, όπως το πρόγραμμα Operation Onymous, έχει οδηγήσει σε επιτυχημένες επιδρομές και κλείσιμο μεγάλων παράνομων αγορών.

Ωστόσο, οι εγκληματίες προσαρμόζονται συνεχώς, χρησιμοποιώντας νέες τεχνικές κρυπτογράφησης και αποκεντρωμένες πλατφόρμες, καθιστώντας τον κυβερνοπόλεμο στο Dark Web μια συνεχή μάχη μεταξύ αρχών και παρανόμων.

Προκλήσεις και περιορισμοί στην αστυνόμευση του Dark Web.

Οι νομικοί περιορισμοί αποτελούν ένα από τα μεγαλύτερα εμπόδια στην αστυνόμευση του Dark Web. Δεδομένου ότι το διαδίκτυο δεν γνωρίζει σύνορα, οι εγκληματίες μπορούν να δραστηριοποιούνται από χώρες με χαλαρό νομικό πλαίσιο, όπου η διαδικτυακή εγκληματικότητα δεν διώκεται αυστηρά. Οι διεθνείς διωκτικές αρχές, όπως το FBI και η Europol, πρέπει να συνεργάζονται με τοπικές αρχές, κάτι που συχνά καθυστερεί τις έρευνες. Επιπλέον, η νομιμότητα ορισμένων τεχνικών επιτήρησης, όπως η χρήση malware για την αποκάλυψη των πραγματικών διευθύνσεων IP των χρηστών, μπορεί να αμφισβητηθεί στα δικαστήρια, θέτοντας εμπόδια στη συλλογή αποδεικτικών στοιχείων.

Από τεχνική άποψη, οι εγκληματίες αναπτύσσουν συνεχώς νέες μεθόδους απόκρυψης για να διαφεύγουν από τις αρχές. Η χρήση end-to-end κρυπτογράφησης σε συνομιλίες και συναλλαγές αποτρέπει την υποκλοπή δεδομένων, ενώ αποκεντρωμένες πλατφόρμες και υπηρεσίες φιλοξενίας που δεν απαιτούν ταυτοποίηση επιτρέπουν τη συνεχή μετεγκατάσταση παράνομων αγορών. Ακόμα και όταν οι αρχές καταφέρνουν να κλείσουν μια αγορά, νέες εμφανίζονται γρήγορα, συχνά με βελτιωμένες μεθόδους ασφαλείας.

Η έλλειψη εξειδικευμένου προσωπικού στις αρχές επιβολής του νόμου αποτελεί έναν ακόμη σημαντικό περιορισμό. Οι έρευνες στο Dark Web απαιτούν ειδικές γνώσεις στον προγραμματισμό, την ανάλυση δεδομένων και την κρυπτογράφηση, δεξιότητες που συνήθως διαθέτουν μόνο εξειδικευμένοι ερευνητές στον ιδιωτικό τομέα. Παράλληλα, οι ηθικοί προβληματισμοί γύρω από την παρακολούθηση του διαδικτύου εγείρουν ζητήματα προστασίας προσωπικών δεδομένων, καθώς οι μέθοδοι που χρησιμοποιούνται για τον εντοπισμό εγκληματιών θα μπορούσαν να επηρεάσουν και αθώους χρήστες.

Συμπεράσματα και μελλοντικές προοπτικές

Συνοπτική ανασκόπηση των βασικών σημείων

Το Dark Web είναι ένα κρυφό κομμάτι του διαδικτύου που δεν είναι προσβάσιμο μέσω παραδοσιακών μηχανών αναζήτησης και απαιτεί εξειδικευμένα δίκτυα όπως το Tor, I2P και Freenet για την πρόσβαση. Παρέχει αυξημένη ανωνυμία και χρησιμοποιείται τόσο για νόμιμους όσο και για παράνομους σκοπούς.

Οι θετικές χρήσεις του περιλαμβάνουν την προστασία της ιδιωτικότητας, την ελευθερία του λόγου, την προστασία πληροφοριοδοτών (Whistleblowers) και την πρόσβαση σε πληροφορίες από χώρες με λογοκρισία. Αντίθετα, το Dark Web έχει συνδεθεί με εγκληματικές δραστηριότητες, όπως το εμπόριο ναρκωτικών, την πώληση όπλων, την εμπορία ανθρώπων και το ξέπλυμα χρήματος.

Οι επικοινωνίες στο Dark Web βασίζονται σε πρωτόκολλα ανωνυμίας, όπως το Onion Routing (που χρησιμοποιείται στο Tor) και το Garlic Routing (που χρησιμοποιείται στο I2P). Οι συναλλαγές πραγματοποιούνται σχεδόν αποκλειστικά μέσω κρυπτονομισμάτων, με κυριότερα το Bitcoin (BTC), Monero (XMR) και Litecoin (LTC), λόγω της ανωνυμίας και της ασφάλειάς τους.

Τέλος, αν και οι αρχές επιβολής του νόμου προσπαθούν να περιορίσουν την εγκληματικότητα στο Dark Web, η χρήση κρυπτογραφίας και αποκεντρωμένων δικτύων καθιστά τον εντοπισμό δραστηριοτήτων ιδιαίτερα δύσκολο, δημιουργώντας προκλήσεις για τη ρύθμισή του.

Πιθανές εξελίξεις στο Dark Web και την κυβερνοασφάλεια

Το Dark Web εξελίσσεται συνεχώς, επηρεαζόμενο από τεχνολογικές και νομοθετικές αλλαγές. Στο μέλλον, αναμένεται να δούμε βελτιώσεις στην ανωνυμία, την ανάπτυξη νέων τεχνικών κρυπτογράφησης και πιθανές προσπάθειες ρύθμισης από κυβερνήσεις και διωκτικές αρχές.

α. Ενίσχυση της Ανωνυμίας. Με την πρόοδο της κβαντικής κρυπτογράφησης και των αποκεντρωμένων δικτύων, οι χρήστες του Dark Web θα έχουν ακόμα μεγαλύτερη προστασία. Νέα πρωτόκολλα απορρήτου, όπως οι αναβαθμισμένες εκδόσεις του Tor και του I2P, θα βελτιώσουν την ασφάλεια των επικοινωνιών.

β. Εξέλιξη των Κρυπτονομισμάτων. Το Monero (XMR) και άλλα ανώνυμα νομίσματα θα γίνουν πιο δημοφιλή, καθώς οι κυβερνήσεις επιδιώκουν να παρακολουθούν το Bitcoin (BTC). Παράλληλα, η ανάπτυξη αποκεντρωμένων ανταλλακτηρίων (DEX) θα καταστήσει ακόμα πιο δύσκολο τον έλεγχο των παράνομων συναλλαγών.

γ. Αυξημένη Παρακολούθηση και Ρυθμίσεις. Οι διωκτικές αρχές χρησιμοποιούν όλο και πιο εξελιγμένα εργαλεία, όπως η τεχνητή νοημοσύνη (AI) και το machine learning, για την παρακολούθηση του Dark Web. Νέοι νόμοι, όπως η υποχρεωτική καταγραφή συναλλαγών κρυπτονομισμάτων, θα στοχεύσουν στη μείωση της εγκληματικότητας.

δ. Βελτιωμένες Μέθοδοι Κυβερνοασφάλειας. Οι εταιρείες και οι χρήστες θα στραφούν σε ισχυρότερες μεθόδους προστασίας δεδομένων, όπως Zero Trust Architecture και αντι-DDoS τεχνικές, για να προστατευθούν από επιθέσεις που προέρχονται από το Dark Web.

Το μέλλον του Dark Web θα εξαρτηθεί από τη μάχη μεταξύ απορρήτου και επιβολής του νόμου, καθώς και από την πρόοδο της τεχνολογίας κυβερνοασφάλειας.

Αναφορές

[1]	(2019). WLEARN: Τι είναι το Σκοτεινό Διαδίκτυο (Dark Web) και πως μπορεί κάποιος να αποκτήσει πρόσβαση σε αυτό. Ανακτήθηκε από: **https://www.wlearn.gr/index.php/articles/1391-what-is-dark**
[2]	(2023). Fivecast - The Dark Web Defined. Ανακτήθηκε από: https://www.fivecast.com/blog/the-dark-web-defined/
[3]	(2022) Spiceworks - Dark Web vs. Deep Web: 5 Key Differences. Ανακτήθηκε από: https://www.spiceworks.com/it-security/security-general/articles/darkweb-vs-deep-web/.
[4]	CIS - Election Security Spotlight – The Surface Web, Dark Web, and Deep Web. Ανακτήθηκε από: https://www.cisecurity.org/insights/spotlight/cybersecurityspotlight-the-surface-web-dark-web-and-deep-web
[5]	(2020) Cyberprotection Magazine. - Darkweb & Internet Anonymity: Exploring The Hidden Internet. Ανακτήθηκε από: https://cyberprotectionmagazine.com/darkweb-internet-anonymity-exploring-the-hidden-internet.
[6]	(2024) AVAST - The Dark Web Browser: What Is Tor, Is it Safe, and How Do You Use It? Ανακτήθηκε από: https://www.avast.com/c-tor-dark-web-browser .
[7]	(2024). Medium - What is the Dark Web: Understanding Its Layers, Risks, and Uses. Ανακτήθηκε από: https://medium.com/@tahirbalarabe2/exploring-thedark-web-understanding-its-layers-risks-and-uses-03409a30fa57
[8]	DSA - Digital Services Act (DSA) | Updates, Compliance. Ανακτήθηκε από: https://www.eu-digital-services-act.com/
[9]	(2017). Congress.gov - H.R.1865 - Allow States and Victims to Fight Online Sex Trafficking Act of 2017. Ανακτήθηκε από: https://www.congress.gov/bill/115thcongress/house-bill/1865/text
[10]	(2023) OnlineSim - What is I2P and how it works? Knowledge base on OnlineSim. Ανακτήθηκε από: https://onlinesim.io/instructions/the-dark-side-ofthe-internet-part-4-what-is-i2p-and-how-it-works?utm_referrer=https://www.google.com/
[11]	(2024) Snatika - Advantages of The Dark Web. Ανακτήθηκε από: https://snatika.com/single-blog/advantages-of-the-dark-web
[12]	(2023) FindLaw - Dark Web Crimes. Ανακτήθηκε από: https://www.findlaw.com/criminal/criminal-charges/dark-web-crimes.html
[13]	ERMProtect - How Criminals Use the Dark Web for Illicit Activities. Ανακτήθηκε από: https://ermprotect.com/blog/dark-web-cybercrime-central/

[14]	(2023) LinkedIn - The Dark Web and Cryptocurrencies: Understanding the Role of Bitcoin. Ανακτήθηκε από: https://www.linkedin.com/pulse/dark-webcryptocurrencies-understanding-role-bitcoin-jayant-dusane
[15]	Bitpanda - What is the Darknet and what does it have to do with Bitcoin? Ανακτήθηκε από: https://www.bitpanda.com/academy/en/lessons/what-is-thedarknet-and-what-does-it-have-to-do-with-bitcoin/
[16]	(2025) – Webion - Εργαλεία Επιτήρησης του Dark Web: Τεχνολογίες και Προκλήσεις. Ανακτήθηκε από: https://webion.gr/ergalia-epitirishw-dark-webteck/.

Βιογραφικό συντάκτη

Ο Υπολοχαγός (ΔΒ) Ραϊόπουλος Θεόδωρος αποφοίτησε από τη Στρατιωτική Σχολή Ευελπίδων (ΣΣΕ) το 2017, ως Ανθυπολοχαγός (ΔΒ). Έχει ολοκληρώσει όλα τα προβλεπόμενα στο βαθμό του σχολεία και έχει αποφοιτήσει επιτυχώς το 2025 από το Τμήμα Αναλυτών / Προγραμματιστών της ΣΠΗΥ. Είναι κάτοχος MSc του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων (Πανεπιστήμιο Αιγαίου-Πολυτεχνική Σχολή) με τίτλο «Πληροφοριακά και Επικοινωνιακά Συστήματα» . Φοίτησε στο Τμήμα Αναλυτών / Προγραμματιστών της Σχολής Προγραμματιστών Ηλεκτρονικών Υπολογιστών του Στρατού Ξηράς, από το οποίο αποφοίτησε επιτυχώς το 2025.

Open Data: Δυνατότητες Και Περιορισμοί Της Επαυξημένης Πραγματικότητας

Λγός (ΔΒ) Δημοσθένης Στατήρας

Εισαγωγή

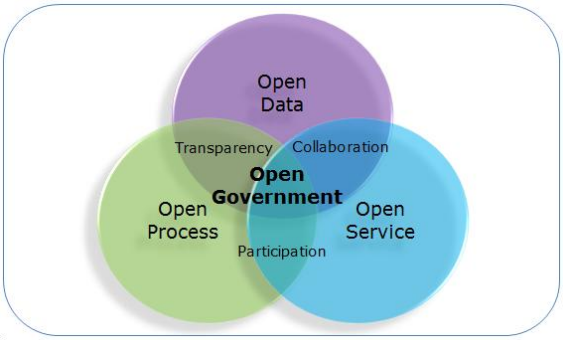
Η θεμελίωση της έννοιας των ανοικτών δεδομένων βασίζεται σε θεωρίες της διακυβέρνησης, της πληροφορίας και της τεχνολογίας. Στο πλαίσιο αυτό, οι εργασίες των Janssen et al. (2012) και Ubaldi (2013) αποτελούν σημαντικές αναφορές, καθώς αναλύουν το ρόλο της διαφάνειας και της συμμετοχής των πολιτών μέσω της ελεύθερης διανομής των δεδομένων.

Σύμφωνα με τον Kitchin (2014), η επανάσταση των δεδομένων οδηγεί σε μια νέα εποχή στην οποία η πληροφόρηση μετατρέπεται σε βασικό πόρο για την καινοτομία και την ανάπτυξη. Τα ανοικτά δεδομένα θεωρούνται ως καταλύτης για την ανάπτυξη και την υποστήριξη νέων επιχειρηματικών μοντέλων, ιδιαίτερα στον τομέα της ψηφιακής καινοτομίας. Η δυνατότητα επαναχρησιμοποίησης των δεδομένων επιτρέπει στους ερευνητές και τους επιχειρηματίες να δημιουργήσουν νέες εφαρμογές που βελτιώνουν την ποιότητα ζωής και προωθούν την ανταγωνιστικότητα της αγοράς (Zuiderwijk & Janssen, 2014). Από την άλλη πλευρά, η θεωρητική συζήτηση επισημαίνει και τους περιορισμούς που συνδέονται με την ποιότητα, την ασφάλεια και την ιδιωτικότητα των δεδομένων. Ορισμένες έρευνες τονίζουν ότι η έλλειψη σαφών προτύπων για την δημοσίευση και διαχείριση των δεδομένων μπορεί να οδηγήσει σε δυσλειτουργίες και να μειώσει την αξιοπιστία τους (Bertot, Jaeger & Grimes, 2010).

Μια άλλη θεωρητική διάσταση αφορά τη σύνδεση των ανοικτών δεδομένων με την ψηφιακή δημοκρατία. Οι Dawes (2009) και Kassen (2013) επισημαίνουν ότι η διάδοση των δεδομένων αποτελεί προϋπόθεση για την ανάπτυξη μιας κουλτούρας διαφάνειας, όπου οι πολίτες έχουν τη δυνατότητα να παρακολουθούν και να αξιολογούν τις ενέργειες των δημόσιων φορέων. Παράλληλα, ωστόσο, τίθεται το ερώτημα του βαθμού εμπλοκής των πολιτών και της επαρκούς υποστήριξης από τα κράτη για την αποτελεσματική χρήση των δεδομένων.

Η ύπαρξη τεχνικών και οργανωτικών προκλήσεων όπως η δια λειτουργικότητα, η τυποποίηση και η διασφάλιση της ποιότητας των δεδομένων αποτελεί ένα βασικό ζήτημα στο θεωρητικό πλαίσιο των ανοικτών δεδομένων. Τέλος, η ανάλυση του θεωρητικού πλαισίου εντάσσει μια ανασκόπηση των μοντέλων διακυβέρνησης που υποστηρίζουν τη χρήση ανοικτών δεδομένων, αναδεικνύοντας την ανάγκη για συνεκτική πολιτική και συνεργασία μεταξύ των δημοσίων και ιδιωτικών φορέων (Borys, Kos & Özcan, 2013). Η αλληλεπίδραση μεταξύ της τεχνολογίας και της πολιτικής καθορίζει όχι μόνο τις δυνατότητες των ανοικτών δεδομένων αλλά και τους περιορισμούς που πρέπει να αντιμετωπιστούν για να επιτευχθεί μια πλήρης αξιοποίηση τους.

Δυνατότητες των Ανοικτών Δεδομένων



Οι δυνατότητες που προσφέρουν τα ανοικτά δεδομένα είναι πολυδιάστατες και αντικατοπτρίζουν τόσο την τεχνολογική πρόοδο όσο και την αλλαγή της νοοτροπίας στον τρόπο διαχείρισης της πληροφορίας. Καταρχάς, τα ανοικτά δεδομένα αποτελούν βασικό στοιχείο για την προώθηση της διαφάνειας, επιτρέποντας την ελεύθερη ροή πληροφοριών που ενισχύει τη δημοκρατία και τη λογοδοσία των δημοσίων φορέων (Dawes, 2009). Μέσω της διάθεσης δεδομένων σε μορφή που είναι προσβάσιμη και κατανοητή από όλους, επιτυγχάνεται μια αποτελεσματικότερη επικοινωνία μεταξύ κρατικού μηχανισμού και πολιτών.

Μία από τις κυριότερες δυνατότητες είναι η ενίσχυση της καινοτομίας. Οι επιχειρήσεις και οι νεοφυείς εταιρείες (startups) επωφελούνται από την ευρεία διαθεσιμότητα δεδομένων για την ανάπτυξη καινοτόμων λύσεων που βελτιώνουν την ποιότητα ζωής και υποστηρίζουν νέες μορφές ψηφιακής οικονομίας (Kitchin, 2014). Η δυνατότητα πρόσβασης σε δεδομένα σε πραγματικό χρόνο, όπως δεδομένα μετακίνησης και περιβαλλοντικά δεδομένα, επιτρέπει τη δημιουργία έξυπνων εφαρμογών που συμβάλλουν στη βιώσιμη ανάπτυξη των πόλεων και στην αποδοτικότερη διαχείριση πόρων.

Επιπρόσθετα, η διάθεση ανοικτών δεδομένων ενισχύει την ερευνητική δραστηριότητα, διευκολύνοντας την παρακολούθηση κοινωνικών, οικονομικών και περιβαλλοντικών φαινομένων.

Η συλλογή και ανάλυση δεδομένων σε μεγάλης κλίμακας έργα επιτρέπει την εξαγωγή στατιστικών συμπερασμάτων και τη διαμόρφωση πολιτικών που ανταποκρίνονται στις ανάγκες της κοινωνίας (Ubaldi, 2013).

Τέλος, η δυνατότητα δια-λειτουργικότητας των ανοικτών δεδομένων παίζει καθοριστικό ρόλο στην ενίσχυση της συνεργασίας μεταξύ διαφορετικών φορέων. Η υιοθέτηση κοινών προτύπων και η ενσωμάτωση δεδομένων από πολλαπλές πηγές δημιουργούν ένα συνεκτικό οικοσύστημα, που υποστηρίζει τόσο τις δημόσιες όσο και τις ιδιωτικές πρωτοβουλίες και συμβάλλει στη βελτίωση των λειτουργικών διαδικασιών.

Εφαρμογές των Ανοικτών Δεδομένων

Η εφαρμογή των ανοικτών δεδομένων έχει βρει ιδιαίτερη απήχηση σε πολλούς τομείς, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Στον δημόσιο τομέα, τα ανοικτά δεδομένα προωθούν τη διαφάνεια και την ευθύνη, δίνοντας στους πολίτες τη δυνατότητα να παρακολουθούν τις δράσεις των δημοσίων φορέων και να αξιολογούν την αποτελεσματικότητα των παρεχόμενων υπηρεσιών (Janssen, Charalabidis & Zuiderwijk, 2012). Επιπλέον, μέσω της διάθεσης δεδομένων που αφορούν τον προϋπολογισμό, τα έργα και τις πολιτικές, επιτυγχάνεται η δημιουργία ενός ανοικτού διαλόγου μεταξύ πολιτών και κρατικών φορέων, ενισχύοντας την κοινωνική συμμετοχή και τη λογοδοσία.

Στον ιδιωτικό τομέα, οι επιχειρήσεις αξιοποιούν τα ανοικτά δεδομένα για την ανάπτυξη νέων προϊόντων και υπηρεσιών. Με την επαναχρησιμοποίηση αυτών των δεδομένων, δημιουργούνται νέες επιχειρηματικές ευκαιρίες και καινοτόμες εφαρμογές που υποστηρίζουν την ανταγωνιστικότητα και την ανάπτυξη της οικονομίας (Kitchin, 2014).

Παραδείγματα εφαρμογών περιλαμβάνουν πλατφόρμες για την παρακολούθηση της κυκλοφορίας, εφαρμογές για το περιβάλλον, συστήματα για τη διαχείριση αστικών υποδομών και έργα «smart city», όπου τα δεδομένα συμβάλλουν στην αποτελεσματικότερη διαχείριση πόρων και στην παροχή καλύτερων υπηρεσιών στους πολίτες.

Επίσης, ο τομέας της έρευνας και της ακαδημαϊκής κοινότητας εκμεταλλεύεται τα ανοικτά δεδομένα για την εξαγωγή συμπερασμάτων, την ανάπτυξη νέων θεωριών και την επαλήθευση υποθέσεων. Μέσω της πρόσβασης σε ένα ευρύ φάσμα δεδομένων, οι ερευνητές μπορούν να πραγματοποιήσουν συγκριτικές αναλύσεις, να αναπτύξουν νέα μοντέλα πρόβλεψης και να αξιολογήσουν την αποτελεσματικότητα πολιτικών (Zuiderwijk & Janssen, 2014).

Περιορισμοί και Προκλήσεις

Παρά τις πολυάριθμες δυνατότητες, η εφαρμογή των ανοικτών δεδομένων αντιμετωπίζει σημαντικούς περιορισμούς και προκλήσεις. Ένας από τους κύριους περιορισμούς αφορά το ζήτημα της ποιότητας και της ακρίβειας των δεδομένων. Η έλλειψη καθολικών προτύπων για τη συλλογή, αποθήκευση και δημοσίευση των δεδομένων οδηγεί συχνά σε ασυνέπειες, ανακρίβειες και δυσκολίες στην ομογενοποίηση των πληροφοριών (Bertot, Jaeger & Grimes, 2010). Αυτός ο περιορισμός επηρεάζει αρνητικά την αξιοπιστία των δεδομένων και την ικανότητα των χρηστών να εξάγουν αξιόπιστα συμπεράσματα.

Ένα άλλο κρίσιμο ζήτημα είναι η προστασία της ιδιωτικότητας. Η ελεύθερη διάθεση δεδομένων που περιέχουν ευαίσθητες πληροφορίες μπορεί να οδηγήσει σε παραβιάσεις της ιδιωτικότητας και σε κινδύνους για τους πολίτες. Ανεπαρκή μέτρα ασφαλείας και έλλειψη νομοθετικών ρυθμίσεων αποτελούν σημαντικά εμπόδια για την ευρεία υιοθέτηση των ανοικτών δεδομένων (Borys, Kos & Özcan, 2013). Η διαχείριση αυτών των ζητημάτων απαιτεί την ανάπτυξη νέων, αυστηρότερων πλαισίων προστασίας δεδομένων, τα οποία θα εξισορροπούν την ανάγκη για διαφάνεια με την προστασία των προσωπικών πληροφοριών. Επιπλέον, οι τεχνικές προκλήσεις αποτελούν σημαντικό παράγοντα περιορισμού.

Η δια λειτουργικότητα μεταξύ διαφορετικών συστημάτων και η ενσωμάτωση δεδομένων από ποικίλες πηγές απαιτούν την εφαρμογή εξελιγμένων τεχνολογικών λύσεων και την υιοθέτηση κοινών προτύπων. Χωρίς την ανάπτυξη κατάλληλων τεχνικών υποδομών, οι προσπάθειες για την πλήρη αξιοποίηση των ανοικτών δεδομένων μπορούν να παρεμποδίσουν την αποτελεσματική λειτουργία και την ανταπόκριση στις ανάγκες των χρηστών (Dawes, 2009).

Τέλος, η πολιτική βούληση και ο οργανωτικός συντονισμός παίζουν καθοριστικό ρόλο στην επιτυχία των πρωτοβουλιών ανοικτών δεδομένων. Σε πολλές περιπτώσεις, η έλλειψη συνεργασίας μεταξύ δημοσίων και ιδιωτικών φορέων, καθώς και η περιορισμένη χρηματοδότηση, επηρεάζουν αρνητικά την υλοποίηση και τη διατήρηση των συστημάτων ανοικτών δεδομένων. Η ενίσχυση του διαλόγου μεταξύ των εμπλεκόμενων φορέων και η εφαρμογή ολοκληρωμένων πολιτικών διακυβέρνησης είναι απαραίτητες προϋποθέσεις για την αντιμετώπιση αυτών των προκλήσεων.

Συγκριτική Ανάλυση Εφαρμογών και Προοπτικών

Για μια ολοκληρωμένη κατανόηση της πρακτικής αξίας των ανοικτών δεδομένων, είναι χρήσιμο να συγκριθούν παραδείγματα εφαρμογών από διαφορετικούς τομείς.

Στον τομέα της μετακίνησης, για παράδειγμα, εφαρμογές που βασίζονται σε δεδομένα κυκλοφορίας επιτρέπουν στους πολίτες να ενημερώνονται για τις συνθήκες στους δρόμους σε πραγματικό χρόνο, συμβάλλοντας στη μείωση της συμφόρησης και στην εξοικονόμηση χρόνου (Kitchin, 2014). Από την άλλη, σε εφαρμογές περιβαλλοντικής παρακολούθησης, τα ανοικτά δεδομένα προσφέρουν πληροφορίες για την ποιότητα του αέρα, την υδρολογία και τις κλιματικές μεταβολές, βοηθώντας τόσο τους ερευνητές όσο και τους φορείς λήψης αποφάσεων να διαμορφώσουν στοχευμένες πολιτικές.

Η σύγκριση αυτή αποκαλύπτει ότι, ενώ οι εφαρμογές ανοικτών δεδομένων παρέχουν σημαντικά οφέλη, οι προοπτικές βελτίωσης εξαρτώνται σε μεγάλο βαθμό από την ποιότητα της τεχνικής υποδομής και την ύπαρξη συνεκτικών πολιτικών. Η επιτυχής εφαρμογή απαιτεί συνεχή αναβάθμιση των τεχνολογικών συστημάτων και την εκπαίδευση των χρηστών, ώστε να μπορούν να αξιοποιήσουν πλήρως τις δυνατότητες που προσφέρουν τα δεδομένα.

Παράλληλα, η εμπειρία από διάφορες χώρες δείχνει ότι οι διαφορετικές στρατηγικές υλοποίησης και οι τοπικές προκλήσεις διαμορφώνουν σημαντικά τα αποτελέσματα. Για παράδειγμα, οι χώρες που έχουν επενδύσει στην ανάπτυξη κοινών προτύπων και στην ενίσχυση της συνεργασίας μεταξύ δημόσιων και ιδιωτικών φορέων παρουσιάζουν καλύτερα αποτελέσματα στη διαχείριση και αξιοποίηση των ανοικτών δεδομένων (Ubaldi, 2013).

Η συγκριτική ανάλυση αυτή καταδεικνύει ότι η επιτυχία των εφαρμογών εξαρτάται από μια σειρά παραμέτρων που συνδυάζουν τεχνικές, οργανωτικές και πολιτικές διαστάσεις. Ενώ οι δυνατότητες για καινοτομία και οικονομική ανάπτυξη είναι σημαντικές, οι περιορισμοί στην ποιότητα των δεδομένων, την προστασία της ιδιωτικότητας και τη δια-λειτουργικότητα παραμένουν κρίσιμα ζητήματα που πρέπει να αντιμετωπιστούν προκειμένου να επιτευχθεί μια ολιστική και βιώσιμη αξιοποίηση των ανοικτών δεδομένων.

Σύγκριση Βιβλιογραφίας

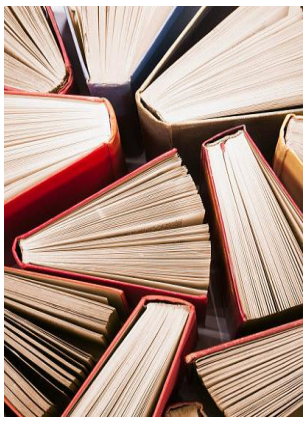
Η βιβλιογραφία για τα ανοικτά δεδομένα παρουσιάζει μια πληθώρα προσεγγίσεων και απόψεων που αντικατοπτρίζουν την πολυπλοκότητα του θέματος. Σε μια πρώτη ανασκόπηση, παρατηρείται ότι οι μελέτες των Janssen et al. (2012) και Ubaldi (2013) εστιάζουν κυρίως στις θετικές επιπτώσεις της διαφάνειας και της συμμετοχής των πολιτών, τονίζοντας την καινοτομία και την οικονομική ανάπτυξη ως κύρια οφέλη.

Αντίθετα, άλλες μελέτες όπως αυτή των Bertot, Jaeger & Grimes (2010) επισημαίνουν τις προκλήσεις που συνδέονται με την προστασία των προσωπικών δεδομένων και την ανάγκη για αυστηρά πλαίσια διακυβέρνησης, καθώς και την πιθανή κατάχρηση των πληροφοριών.

Η σύγκριση των πηγών αποκαλύπτει ότι οι ερευνητές συμφωνούν ως προς τη σημασία της τεχνολογικής υποδομής για την επιτυχή εφαρμογή των ανοικτών δεδομένων, αλλά διαφέρουν ως προς την εκτίμηση των παραγόντων που εμποδίζουν την πλήρη αξιοποίησή τους. Για παράδειγμα, ενώ ο Kitchin (2014) επισημαίνει την ανάγκη για συνεχή αναβάθμιση των συστημάτων και την ενσωμάτωση νέων τεχνολογιών, ο Dawes (2009) εστιάζει περισσότερο στο ρόλο της διακυβέρνησης και της πολιτικής θέλησης για την προώθηση των ανοικτών δεδομένων.

Μια άλλη διάσταση σύγκρισης αφορά την εμπειρική ανάλυση των αποτελεσμάτων των πρωτοβουλιών ανοικτών δεδομένων.

Οι μελέτες που επικεντρώνονται σε περιπτωσιολογικές αναλύσεις, όπως αυτή του Kassen (2013), παρουσιάζουν συγκεκριμένα παραδείγματα επιτυχίας αλλά και αποτυχίας, υπογραμμίζοντας ότι η εφαρμογή των ανοικτών δεδομένων εξαρτάται σε μεγάλο βαθμό από το πλαίσιο και τις τοπικές συνθήκες. Από την άλλη πλευρά, οι θεωρητικές προσεγγίσεις, όπως αυτές των Zuiderwijk & Janssen (2014), προσφέρουν ένα πιο γενικευμένο μοντέλο για την κατανόηση των δυνατοτήτων και περιορισμών, χωρίς να εμβαθύνουν στις λεπτομέρειες κάθε περίπτωσης.



Η σύγκριση της βιβλιογραφίας αποδεικνύει επίσης τη σημασία της χρονικής διάστασης στην εξέλιξη του θέματος. Οι παλαιότερες μελέτες τείνουν να τονίζουν τα αρχικά οφέλη των ανοικτών δεδομένων ως εργαλείο διαφάνειας, ενώ οι πιο σύγχρονες έρευνες εστιάζουν σε πιο πολύπλοκα ζητήματα όπως η ασφάλεια, η ιδιωτικότητα και η δια-λειτουργικότητα των συστημάτων (Löffler, 2017; Smith, 2015). Αυτή η χρονική εξέλιξη των θεωρητικών και εμπειρικών προσεγγίσεων καταδεικνύει τη δυναμική φύση του θέματος και την ανάγκη για συνεχή αναθεώρηση και προσαρμογή των πολιτικών και τεχνολογικών υποδομών.

Συζήτηση Κρίσιμων Θεμάτων

Η ανάλυση των πηγών έρχεται να αναδείξει κάποια κρίσιμα ζητήματα που απαιτούν περαιτέρω διερεύνηση. Ένα από τα πιο σημαντικά είναι το ζήτημα της ποιότητας και αξιοπιστίας των δεδομένων. Παρά τα ανοιχτά οφέλη της προσβασιμότητας, πολλοί ερευνητές επισημαίνουν ότι η έλλειψη συστηματικών προτύπων για τη συλλογή, επεξεργασία και δημοσίευση των δεδομένων μπορεί να οδηγήσει σε ανακρίβειες και παραπλανητικές ερμηνείες (Bertot, Jaeger & Grimes, 2010).

Επιπλέον, το ζήτημα της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας παραμένει επίκαιρο, καθώς η ελεύθερη διάθεση πληροφοριών μπορεί να θέσει σε κίνδυνο την ασφάλεια των πολιτών, ειδικά όταν δεν εφαρμόζονται επαρκή μέτρα ασφαλείας (Borys, Kos & Özcan, 2013).

Ένα άλλο κρίσιμο θέμα αφορά την ενσωμάτωση και τη δια λειτουργικότητα των δεδομένων σε επίπεδο κρατικών δομών και ιδιωτικών φορέων. Οι έρευνες τονίζουν ότι η έλλειψη συντονισμού μεταξύ των διαφόρων φορέων μπορεί να δημιουργήσει απομονωμένα δεδομένα που δεν ανταποκρίνονται στις ανάγκες της σύγχρονης πληροφορίας και τεχνολογίας (Dawes, 2009). Η ανάγκη για ενοποιημένα συστήματα και προσαρμοσμένες πολιτικές διακυβέρνησης είναι θεμελιώδης για την πλήρη αξιοποίηση των δυνατοτήτων των ανοικτών δεδομένων.

Επιπροσθέτως, η διαχείριση των ανοικτών δεδομένων απαιτεί ένα ευρύ φάσμα δεξιοτήτων και τεχνικών γνώσεων, τόσο στον τομέα της πληροφορικής όσο και της διοίκησης. Η εφαρμογή στρατηγικών για την εκπαίδευση και κατάρτιση των εμπλεκόμενων φορέων αποτελεί έναν κρίσιμο παράγοντα για την επιτυχή υλοποίηση των πρωτοβουλιών (Kitchin, 2014). Τέλος, η συζήτηση αναδεικνύει την ανάγκη για έναν συνεχή διάλογο μεταξύ ερευνητών, δημόσιων και ιδιωτικών φορέων, προκειμένου να εντοπιστούν και να επιλυθούν τα προβλήματα που προκύπτουν από την πρακτική εφαρμογή των ανοικτών δεδομένων.

Ομαδοποίηση Πηγών

Η ομαδοποίηση των πηγών μπορεί να γίνει βάσει θεματικών αξόνων, χρονικής ακολουθίας και θεωρητικών προσεγγίσεων. Από θεματική άποψη, οι πηγές χωρίζονται σε εκείνες που εστιάζουν στις δυνατότητες και τα οφέλη των ανοικτών δεδομένων (π.χ. Janssen et al., 2012· Ubaldi, 2013· Kitchin, 2014) και εκείνες που επικεντρώνονται στους περιορισμούς και τις προκλήσεις (π.χ. Bertot, Jaeger & Grimes,2010· Borys, Kos & Özcan, 2013).

Σε ό,τι αφορά την χρονική διάσταση, οι πρώιμες μελέτες (Dawes, 2009) παρουσιάζουν ένα ιδανικό μοντέλο διαφάνειας και συμμετοχής, ενώ οι πιο σύγχρονες έρευνες (Löffler, 2017· Smith, 2015) εντοπίζουν τις σύγχρονες προκλήσεις της ασφάλειας, της ιδιωτικότητας και της δια-λειτουργικότητας. Αυτή η χρονική εξέλιξη επιτρέπει την κατανόηση του τρόπου με τον οποίο οι εξελίξεις στην τεχνολογία και τις πολιτικές μεταβάλλουν την εφαρμογή των ανοικτών δεδομένων.

Τέλος, από θεωρητική σκοπιά, παρατηρείται μια διχοτόμηση μεταξύ των θεωρητικών προσεγγίσεων που βλέπουν τα ανοικτά δεδομένα ως εργαλείο καινοτομίας και οικονομικής ανάπτυξης και εκείνων που επικεντρώνονται στον κοινωνικό και δημοκρατικό αντίκτυπο της διαφάνειας.

Αυτή η ομαδοποίηση βοηθά στην καλύτερη κατανόηση των αλληλοεπιδράσεων μεταξύ τεχνολογικών, πολιτικών και κοινωνικών παραγόντων, δημιουργώντας ένα πλήρες πλέγμα ανάλυσης που μπορεί να αποτελέσει οδηγό για μελλοντικές έρευνες και εφαρμογές.

Συμπεράσματα

Σύνοψη και αξιολόγηση των ευρημάτων

Η παρούσα εργασία ανέλυσε διεξοδικά το πεδίο των ανοικτών δεδομένων, εξετάζοντας τόσο τις δυνατότητες που προσφέρουν όσο και τους περιορισμούς που συνοδεύουν την εφαρμογή τους. Από τη μελέτη του θεωρητικού πλαισίου, προέκυψε ότι τα ανοικτά δεδομένα αποτελούν βασικό παράγοντα για την ενίσχυση της διαφάνειας, την προώθηση της καινοτομίας και την υποστήριξη της ψηφιακής δημοκρατίας (Janssen et al., 2012· Ubaldi, 2013). Τα οφέλη τους είναι πολλαπλά, από τη δημιουργία νέων επιχειρηματικών μοντέλων έως την ενίσχυση της συμμετοχής των πολιτών, ενώ ταυτόχρονα αναδεικνύονται και σημαντικά ζητήματα όπως η προστασία της ιδιωτικότητας και η διασφάλιση της ποιότητας των δεδομένων (Bertot, Jaeger & Grimes, 2010· Borys, Kos & Özcan, 2013).

Η σύγκριση της βιβλιογραφίας αποκάλυψε ότι, παρόλο που οι πρώιμες έρευνες επικεντρώνονταν στις θετικές επιπτώσεις των ανοικτών δεδομένων, οι πιο σύγχρονες προσεγγίσεις εστιάζουν στις τεχνικές και οργανωτικές προκλήσεις που απαιτούν συνεχή βελτίωση και προσαρμογή. Η δια λειτουργικότητα, η τυποποίηση και η εξασφάλιση της ποιότητας αποτελούν κρίσιμα ζητήματα που πρέπει να αντιμετωπιστούν, προκειμένου οι δημόσιοι και ιδιωτικοί φορείς να αξιοποιήσουν πλήρως τις δυνατότητες που προσφέρουν τα ανοικτά δεδομένα (Dawes, 2009· Kassen, 2013).

Η ομαδοποίηση των πηγών βάσει θεματικών αξόνων και χρονικών προσεγγίσεων ανέδειξε την πολυπλοκότητα του θέματος, καθώς και την ανάγκη για διεπιστημονική συνεργασία και συνεχή διάλογο μεταξύ των εμπλεκόμενων φορέων. Σε αυτό το πλαίσιο, γίνεται σαφές ότι η υιοθέτηση ολοκληρωμένων πολιτικών διακυβέρνησης αποτελεί προϋπόθεση για την επιτυχή εφαρμογή και αξιοποίηση των ανοικτών δεδομένων.

Προτάσεις για Μελλοντική Έρευνα

Τέλος, βασιζόμενοι στα ευρήματα της βιβλιογραφικής ανάλυσης, διαπιστώνεται ότι ενώ οι ανοικτές πληροφορίες προσφέρουν μεγάλες δυνατότητες για την προώθηση της διαφάνειας και της καινοτομίας, οι περιορισμοί που σχετίζονται με την ασφάλεια, την ιδιωτικότητα και την τεχνική υποδομή απαιτούν ιδιαίτερη προσοχή και συνεχή προσπάθεια για την ανάπτυξη κατάλληλων λύσεων. Οι μελλοντικές έρευνες θα πρέπει να εστιάσουν στην ανάπτυξη νέων προτύπων και μοντέλων που θα ενισχύσουν την αμοιβαία συνεργασία μεταξύ των δημόσιων και ιδιωτικών φορέων, ενώ παράλληλα θα εξασφαλίζουν τη βιωσιμότητα και την αξιοπιστία των ανοικτών δεδομένων.

Η παρούσα εργασία καταλήγει στο συμπέρασμα ότι η επιτυχής αξιοποίηση των ανοικτών δεδομένων απαιτεί όχι μόνο τεχνικές και τεχνολογικές επενδύσεις, αλλά και μια αλλαγή νοοτροπίας που θα στηρίζεται στη διαφάνεια, τη συμμετοχή και την καινοτομία. Οι προτάσεις για μελλοντική έρευνα περιλαμβάνουν την ενδελεχή ανάλυση των επιπτώσεων των ανοικτών δεδομένων σε τοπικό και διεθνές επίπεδο, καθώς και την ανάπτυξη νέων εργαλείων για τη μέτρηση της ποιότητας και της δια-λειτουργικότητας των δεδομένων.

Αναφορές.

[1]	Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to Create a Culture of Transparency: E-Government and Social Media as Openness and Anti-Corruption Tools for Societies. Government Information Quarterly, 27(3),264-271.
[2]	Borys, D., Kos, D., & Özcan, P. (2013). Open Data: Access, Use, and Applications. Journal of Information Science, 39(4), 453-466.
[3]	Dawes, S. (2009). The Evolution of E-Government to Open Government. Government Information Quarterly, 26(1), 3-8.
[4]	Georgiou, P., & Nikolaidis, N. (2020). Αξιολόγηση της Αποτελεσματικότητας των Ανοικτών Δεδομένων στο Δημόσιο Τομέα. Ελληνική Επιθεώρηση Δημόσιας Διοίκησης, 15(2), 45-60.
[5]	Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits Adoption Barriers and Myths of Open Data and Open Government. Government Information Quarterly, 29(4), 258-268.
[6]	Kassen, M. (2013). A Promising Phenomenon of Open Data: A Case Study of the Danish Open Data Initiative. Government Information Quarterly, 30(4), 476-487.
[7]	Kitchin, R. (2014). The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. Sage Publications, 240 pages.

[8]	Löffler, M. (2017). Open Data in Europe: Policy, Practice and Perspectives. European Policy Analysis, 3(1), 22-35.
[9]	Papadopoulos, T. (2018). Η Διακυβέρνηση των Ανοικτών Δεδομένων στην Ελλάδα. Ελληνικό Περιοδικό Δημόσιας Διοίκησης, 12(3), 112-125.
[10]	Ruijer, E., Grimmelikhuijsen, S., & Meijer, A. (2017). Open data for democracy: Developing a theoretical framework for open data use. Government Information Quarterly, 34(1), 45-52.
[11]	Ubaldi, B. (2013). Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives. OECD Working Papers on Public Governance, No. 22, OECD Publishing, 48 σελίδες.
[12]	Zuiderwijk, A., & Janssen, M. (2014). Open Data Policies, Open Data Use and Open Data Impact: A Review of the Empirical Literature. Government Information Quarterly, 31(1), 17-29.

Βιογραφικό συντάκτη.

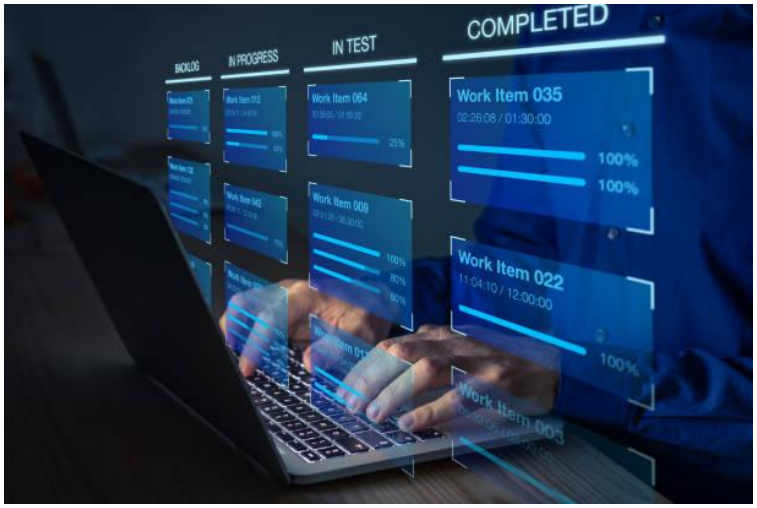
Ο Λγός (ΔΒ) Δημοσθένης Στατήρας αποφοίτησε από τη Στρατιωτική Σχολή Ευελπίδων (ΣΣΕ) το 2015, ως Ανθυπολοχαγός (ΔΒ). Έχει ολοκληρώσει όλα τα προβλεπόμενα στο βαθμό του σχολεία και έχει αποφοιτήσει επιτυχώς το 2025 από το Τμήμα Αναλυτών/Προγραμματιστών της ΣΠΗΥ. Είναι απόφοιτος του Μεταπτυχιακού Προγράμματος «Πληροφορική» και κάτοχος πιστοποιήσεων CCNA και CCNA Instructor. Παράλληλα δραστηριοποιείται ως εκπαιδευτής δικτύων και ακαδημαϊκός συνεργάτης στο City Unity College. Συμμετέχει ενεργά σε ερευνητικά και τεχνολογικά έργα που αφορούν τη βελτίωση επιχειρησιακών διαδικασιών και τη χρήση τεχνητής νοημοσύνης σε περιβάλλοντα άμυνας και εκπαίδευσης.

Μέθοδοι δοκιμής λογισμικού και συγκριτική αξιολόγηση τους.

Ανθχος (Ε) Δημήτριος Γουλόπουλος

Εισαγωγή

Στον σύγχρονο κόσμο, όπου η τεχνολογία έχει ενσωματωθεί σε κάθε έκφανση της ανθρώπινης δραστηριότητας, το λογισμικό αποτελεί θεμέλιο λίθο για τη λειτουργία της κοινωνίας. Εφαρμογές που σχετίζονται με τραπεζικές υπηρεσίες, ιατρικά συστήματα και τη διαχείριση κρίσιμων υποδομών εξαρτώνται από την ορθή και απρόσκοπτη λειτουργία των πληροφοριακών συστημάτων. Συνεπώς, η ανάπτυξη λογισμικού υψηλής ποιότητας δεν είναι απλώς επιθυμητή — είναι επιτακτική ανάγκη.



Η διαδικασία του ελέγχου λογισμικού (BrowserStack, 2025) αποτελεί αναπόσπαστο στάδιο κατά την ανάπτυξη μιας εφαρμογής, καθώς διασφαλίζει ότι το λογισμικό ανταποκρίνεται στις καθορισμένες απαιτήσεις και προσδοκίες. Με άλλα λόγια, πρόκειται για μια συστηματική μέθοδο αξιολόγησης και επιβεβαίωσης της σωστής λειτουργίας ενός συστήματος, τόσο σε τεχνικό όσο και σε λειτουργικό επίπεδο. Μέσω αυτής της διαδικασίας εντοπίζονται σφάλματα, δυσλειτουργίες και πιθανές αδυναμίες, εξασφαλίζοντας την ποιότητα και την αξιοπιστία του τελικού προϊόντος.

Καθώς τα πληροφοριακά συστήματα αναλαμβάνουν όλο και πιο κρίσιμες λειτουργίες — από την υγειονομική περίθαλψη μέχρι την οικονομική δραστηριότητα και την εκπαίδευση — η ανάγκη για πλήρες και αποδοτικό testing γίνεται ολοένα και πιο έντονη. Σφάλματα στο λογισμικό ενδέχεται να προκαλέσουν σημαντικές οικονομικές απώλειες ή ακόμη και να θέσουν σε κίνδυνο την ανθρώπινη ζωή.

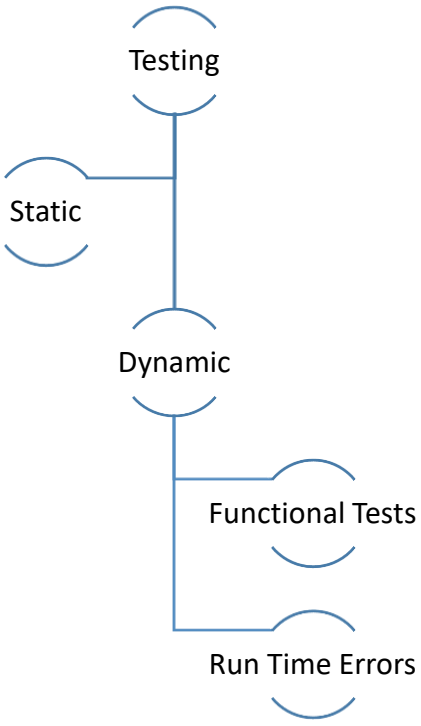
Στο παρόν δοκίμιο εξετάζονται οι κυριότερες μέθοδοι ελέγχου λογισμικού, με ανάλυση των χαρακτηριστικών τους και σύγκριση των πλεονεκτημάτων και των περιορισμών που παρουσιάζουν. Στόχος είναι να αποτυπωθεί μια σφαιρική εικόνα των διαθέσιμων στρατηγικών, συμβάλλοντας έτσι στη βελτιστοποίηση της ποιότητας και της αξιοπιστίας των πληροφοριακών συστημάτων.

Κατηγοριοποίηση Μεθόδων Δοκιμών

Το στατικό και το δυναμικό testing αποτελούν δύο βασικές κατηγορίες δοκιμών λογισμικού, οι οποίες διαφέρουν ως προς τη μέθοδο εφαρμογής και τα αποτελέσματα που παρέχουν. (Gobo, 2025)

Στατική και Δυναμική Δοκιμή

Το στατικό testing αναφέρεται στη διαδικασία ελέγχου του λογισμικού χωρίς την εκτέλεση του κώδικα. Περιλαμβάνει τεχνικές όπως η ανασκόπηση κώδικα (code review), η επιθεώρηση εγγράφων σχεδιασμού και η χρήση εργαλείων στατικής ανάλυσης. Στόχος του στατικού testing είναι να εντοπίσει σφάλματα, κενά λογικής και παραβάσεις προτύπων ανάπτυξης σε πρώιμα στάδια του κύκλου ζωής του λογισμικού. Το κύριο πλεονέκτημα του στατικού testing είναι η δυνατότητα ανίχνευσης λαθών σε πρώιμο στάδιο, γεγονός που μειώνει σημαντικά το κόστος διόρθωσης.



Βασικές τεχνικές είναι:

- Code Reviews: Συστηματικός έλεγχος του πηγαίου κώδικα από μία ή περισσότερες ομάδες ανάπτυξης για την ανίχνευση σφαλμάτων, αδυναμιών και αποκλίσεων από τις προδιαγραφές.
- Static Analysis: Χρήση αυτοματοποιημένων εργαλείων που αναλύουν τον κώδικα για την εύρεση πιθανών σφαλμάτων χωρίς την εκτέλεσή του.

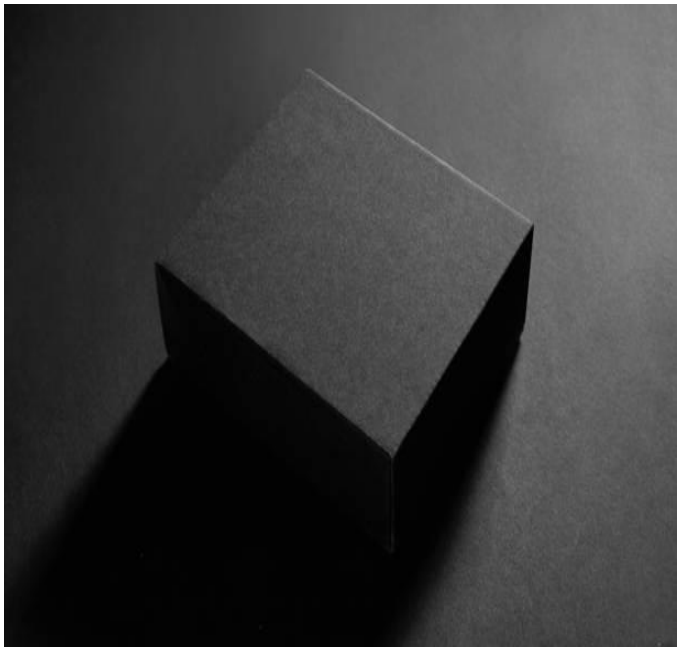
Το δυναμικό testing περιλαμβάνει την εκτέλεση του λογισμικού με στόχο τον εντοπισμό σφαλμάτων που προκύπτουν κατά τη διάρκεια της λειτουργίας του. Εξετάζει τη συμπεριφορά του συστήματος σε πραγματικές ή προσομοιωμένες συνθήκες, αξιολογώντας αν πληρούνται οι λειτουργικές και μη λειτουργικές απαιτήσεις. Βασικές τεχνικές είναι:

- Λειτουργικές Δοκιμές (Functional Tests): Έλεγχος αν το σύστημα εκτελεί σωστά τις απαιτούμενες λειτουργίες.
- Ανίχνευση Run-Time Σφαλμάτων: Καταγραφή και αξιολόγηση σφαλμάτων που εμφανίζονται κατά τη λειτουργία του λογισμικού, όπως memory leaks, crashes και λογικά σφάλματα.

Δοκιμή βάσει γνώσης του κώδικα

Black Box Testing

Το Black Box Testing (checkpoint, 2025) επικεντρώνεται στον έλεγχο της λειτουργικότητας του λογισμικού χωρίς γνώση του εσωτερικού κώδικα ή της εσωτερικής δομής του συστήματος. Ο ελεγκτής δίνει εισόδους στο σύστημα και παρατηρεί τις εξόδους, χωρίς να ενδιαφέρεται για τον τρόπο με τον οποίο παράγονται. Πλεονεκτήματα είναι η εύκολη εφαρμογή από άτομα χωρίς τεχνικές γνώσεις και ότι είναι κατάλληλο για τελικούς χρήστες και αποδοχή προϊόντος. Ενώ μειονέκτημα του είναι ότι δεν μπορεί να εντοπίσει εσωτερικά σφάλματα ή λογικές αστοχίες στον κώδικα.



White Box Testing

Το White Box Testing προϋποθέτει πλήρη γνώση του εσωτερικού κώδικα και της λογικής ροής του λογισμικού. Ο ελεγκτής σχεδιάζει δοκιμές που καλύπτουν όλες τις πιθανές διαδρομές, τις συνθήκες και τις ροές ελέγχου μέσα στο πρόγραμμα. Πλεονεκτήματα του είναι η κάλυψη της λογικής του λογισμικού και ο εντοπισμός λογικών σφαλμάτων. Αντίθετα απαιτεί μεγάλο χρονικό διάστημα και τεχνικές γνώσεις ενώ ταυτόχρονα είναι δύσκολο να εφαρμοστεί σε μεγάλα και πολύπλοκα συστήματα.

Gray Box Testing

Το Gray Box Testing αποτελεί έναν συνδυασμό των δύο προηγούμενων μεθόδων. Ο ελεγκτής έχει μερική γνώση της εσωτερικής δομής του συστήματος, γεγονός που επιτρέπει στοχευμένο έλεγχο των κρίσιμων περιοχών. Χαρακτηριστικό είναι ότι εφαρμόζεται συνήθως από testers που έχουν πρόσβαση σε τεχνικές λεπτομέρειες, αλλά δεν επεμβαίνουν άμεσα στον κώδικα. Βασικά πλεονεκτήματα είναι ο εντοπισμός θεμάτων σχετικά με την ασφάλεια και ενσωμάτωση.

Functional και Non-Functional Testing

Η δοκιμή λογισμικού χωρίζεται σε δύο μεγάλες κατηγορίες με βάση το είδος των απαιτήσεων που εξετάζονται: το Functional Testing και το Non-Functional Testing. Κάθε κατηγορία καλύπτει διαφορετικές πτυχές της ποιότητας του λογισμικού και απαιτεί διαφορετικές τεχνικές και στρατηγικές.

Functional Testing

Το Functional Testing έχει ως στόχο να επαληθεύσει ότι μια εφαρμογή εκτελεί σωστά τις λειτουργίες για τις οποίες έχει σχεδιαστεί. Για παράδειγμα, οι λειτουργικές δοκιμές μπορεί να ελέγχουν τον μηχανισμό ταυτοποίησης μιας εφαρμογής, ώστε να διαπιστωθεί ότι οι έγκυροι χρήστες μπορούν να συνδεθούν επιτυχώς, ενώ οι μη έγκυρες προσπάθειες σύνδεσης απορρίπτονται.

Οι βασικές μορφές λειτουργικού testing περιλαμβάνουν:

- Sanity Checks (Γρήγοροι έλεγχοι ορθότητας): Βασικές δοκιμές για να επιβεβαιωθεί ότι ένα σύστημα λειτουργεί μετά από μικρές αλλαγές.

• Integration Testing (Δοκιμή Ενσωμάτωσης): Έλεγχος της συνεργασίας μεταξύ διαφορετικών ενοτήτων λογισμικού.

• System Testing (Δοκιμή Συστήματος): Έλεγχος της πλήρους λειτουργικότητας του συστήματος ως σύνολο.

Η λειτουργική δοκιμή είναι κρίσιμη για τη διασφάλιση ότι κάθε χαρακτηριστικό και κάθε διαδικασία της εφαρμογής συμπεριφέρεται ακριβώς όπως αναμένεται, παρέχοντας στον χρήστη μια ασφαλή και ομαλή εμπειρία.

Τύποι Functional Testing

1. Unit Testing: Οι προγραμματιστές δημιουργούν και εκτελούν δοκιμές μονάδας για μεμονωμένα τμήματα κώδικα πριν αυτά ενσωματωθούν στο μεγαλύτερο έργο.
2. Component Testing (Δοκιμή Συστατικών):Η δοκιμή συστατικών απομονώνει και ελέγχει μεμονωμένες μονάδες λογισμικού για εντοπισμό σφαλμάτων.
3. Integration Testing: Μετά την επαλήθευση των επιμέρους συστατικών, αυτά ενσωματώνονται και δοκιμάζονται από κοινού για συλλογική λειτουργικότητα.
4. System Testing: Έλεγχος της λειτουργικότητας ολόκληρου του συστήματος .(πχ.test λειτουργικότητας ενός e-shop κάνοντας παραγγελία.)
5. Regression Testing: Η δοκιμή παλινδρόμησης διασφαλίζει ότι οι αλλαγές στο λογισμικό δεν παρεμβαίνουν στην υπάρχουσα λειτουργικότητα.
6. Sanity Testing: Η δοκιμή ορθότητας επαληθεύει τη σταθερότητα μιας νέας έκδοσης μετά από διορθώσεις σφαλμάτων ή προσθήκη νέου κώδικα.

7. Smoke Testing: Η δοκιμή καπνού εκτελείται από το τμήμα Ποιοτικού Ελέγχου (QA) αμέσως μετά την ολοκλήρωση της κατασκευής (build) για τον έλεγχο κρίσιμων λειτουργιών.
8. Acceptance Testing: Διασφαλίζει ότι η βασική λειτουργικότητα του λογισμικού είναι άθικτη πριν από περαιτέρω δοκιμές ή την επίσημη κυκλοφορία.

Παράδειγμα Functional Testing

Ας δούμε ένα πρακτικό παράδειγμα λειτουργικών δοκιμών σε μια εφαρμογή υγείας (BroswerStack, 2025). Μια εφαρμογή υγείας (healthcare app) αποφασίζει να προσθέσει τη δυνατότητα κατ' οικον. παράδοσης φαρμάκων. Ένα από τα βασικά χαρακτηριστικά είναι το κουμπί "Προσθήκη στο Καλάθι". Για να διασφαλιστεί ότι το κουμπί λειτουργεί σωστά, εκτελείται δοκιμή μονάδας (unit test), η οποία ελέγχει την εγκυρότητα και τη σωστή απόκριση του μεμονωμένου κουμπιού.

Παράλληλα, η εφαρμογή επιθυμεί να εμφανίζει στους χρήστες κοντινά κέντρα υγείας με βάση τα δεδομένα GPS. Η επαλήθευση αυτής της λειτουργίας απαιτεί δοκιμή συστατικού (component test), καθώς εμπλέκονται πολλές μονάδες που πρέπει να συνεργαστούν (π.χ. μονάδα GPS, μονάδα χάρτη, μονάδα βάσης δεδομένων) για την επίτευξη του επιθυμητού αποτελέσματος. Επιπλέον, η εφαρμογή προσφέρει στους χρήστες τη δυνατότητα άμεσης μεταφοράς χρημάτων από τον τραπεζικό τους λογαριασμό στο ηλεκτρονικό πορτοφόλι της εφαρμογής, για ταχύτερες αγορές. Σε αυτό το σημείο εμπλέκονται δύο διαφορετικές μονάδες (bank API και wallet module), και απαιτείται η εκτέλεση δοκιμής ενσωμάτωσης (integration test) για την επαλήθευση της σωστής συνεργασίας και λειτουργίας τους.

Non-Functional Testing

Το Non-Functional Testing αξιολογεί την απόδοση, τη χρηστικότητα και άλλα χαρακτηριστικά μιας εφαρμογής λογισμικού, πέρα από τις βασικές της λειτουργίες. Στόχος του είναι να διασφαλίσει ότι το λογισμικό πληροί τα πρότυπα ποιότητας όσον αφορά την ταχύτητα, την ασφάλεια και την επεκτασιμότητα.

Όπως δηλώνει και το όνομά του, το μη λειτουργικό testing καλύπτει τα χαρακτηριστικά εκείνα του λογισμικού που δεν σχετίζονται άμεσα με τη λειτουργικότητα, αλλά με τον τρόπο που η λειτουργικότητα παραδίδεται στον χρήστη. Ελέγχει όλα όσα δεν έχουν ήδη επαληθευτεί μέσω των λειτουργικών δοκιμών. Τα μη λειτουργικά χαρακτηριστικά του λογισμικού περιλαμβάνουν:

- Απόδοση (Performance)
- Χρηστικότητα (Usability)
- Σταθερότητα (Stability)
- Αποδοτικότητα (Efficiency)
- Συντηρησιμότητα (Maintainability)
- Φορητότητα (Portability)

Ο τελικός στόχος του Non-Functional Testing είναι να βελτιστοποιήσει όλα τα μη λειτουργικά χαρακτηριστικά, ώστε το λογισμικό που δοκιμάζεται να προσφέρει την καλύτερη δυνατή εμπειρία χρήστη.

Τύποι Non-Functional Testing

α) Performance Testing: Έλεγχος ταχύτητας και αποδοτικότητας υπό φορτίο.(πχ. μέτρηση ταχύτητας με χιλιάδες χρήστες ταυτόχρονα)

β) Security Testing: Έλεγχος ανθεκτικότητας σε επιθέσεις και παραβιάσεις.

γ) Usability Testing: Έλεγχος ευκολίας χρήσης από τον τελικό χρήστη.

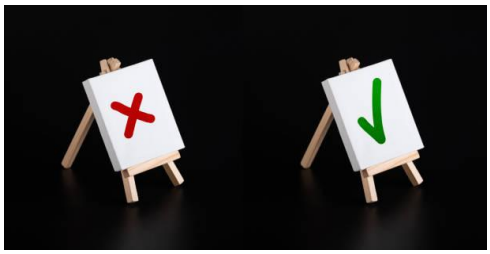
δ) Compatibility Testing: Έλεγχος συμβατότητας με διάφορες πλατφόρμες και περιβάλλοντα.(πχ. Mobile app)

Βασικές Διαφορές Functional και Non-Functional Testing

Χαρακτηριστικό	**Functional Testing**	**Non-Functional Testing**
Εστίαση	Λειτουργικότητα	Απόδοση, ασφάλεια, χρηστικότητα
Ερώτηση	"Κάνει το σωστό;"	"Το κάνει σωστά και αποδοτικά;"
Τεχνικές	Black Box, Requirement-based Testing	Load, Stress, Usability, Security Testing

Παραδείγματα	Ορθές έξοδοι, σωστή εκτέλεση διαδικασιών	Γρήγορη απόκριση, προστασία δεδομένων

Σχέση Functional και Non-Functional Testing



Η πλήρης αξιολόγηση ενός πληροφοριακού συστήματος απαιτεί τη συνδυασμένη εφαρμογή τόσο των λειτουργικών όσο και των μη λειτουργικών δοκιμών (Requiment, 2025). Το γεγονός ότι ένα λογισμικό εκτελεί σωστά τις βασικές του λειτουργίες δεν σημαίνει απαραίτητα πως είναι και αποτελεσματικό ή αξιόπιστο στο σύνολό του. Ζητήματα όπως η χαμηλή ταχύτητα, η κακή εμπειρία χρήστη ή οι αδυναμίες ασφαλείας — τα οποία ελέγχονται μέσω Non-Functional Testing — μπορεί να οδηγήσουν στην απόρριψη του προϊόντος από τους τελικούς χρήστες.

Για παράδειγμα, μια τραπεζική εφαρμογή μπορεί να διεκπεραιώνει με ακρίβεια τις συναλλαγές (λειτουργικά σωστή), αλλά αν καθυστερεί υπερβολικά κατά τη σύνδεση, όπως όταν απαιτούνται 20 δευτερόλεπτα για να φορτώσει, τότε αποτυγχάνει σε επίπεδο απόδοσης. Μια τέτοια υστέρηση ενδέχεται να αποθαρρύνει τους χρήστες και να επηρεάσει αρνητικά τη φήμη και τη χρήση της εφαρμογής.

Σύγχρονες Τάσεις στο Software Testing

Το πεδίο του software testing έχει εξελιχθεί ραγδαία τα τελευταία χρόνια, υπό την πίεση της αυξανόμενης πολυπλοκότητας των συστημάτων και των απαιτήσεων για ταχύτατες κυκλοφορίες προϊόντων στην αγορά. Νέες μέθοδοι και τεχνολογίες (Trymata, n.d.) έχουν εμφανιστεί, κάνοντας τη διαδικασία πιο αποδοτική και αποτελεσματική.

Αυτοματοποίηση Δοκιμών (Test Automation)

Η αυτοματοποίηση αποτελεί πλέον αναπόσπαστο μέρος της διαδικασίας δοκιμής λογισμικού και θεωρείται θεμελιώδης στρατηγική στη σύγχρονη ανάπτυξη εφαρμογών (Zaptest, n.d.). Με την ταχεία εξέλιξη της τεχνολογίας και την αυξανόμενη πολυπλοκότητα των πληροφοριακών συστημάτων, η ανάγκη για ταχύτερες και πιο αποδοτικές δοκιμές έχει οδηγήσει στην ευρεία υιοθέτηση αυτοματοποιημένων μεθόδων.

Η χρήση εξειδικευμένων εργαλείων όπως τα Selenium, Cypress, JUnit και TestNG (Hamilton, 2024) επιτρέπει την καταγραφή και επανάληψη σεναρίων δοκιμών χωρίς την ανάγκη συνεχούς ανθρώπινης παρέμβασης.

Μέσω αυτών των εργαλείων, οι προγραμματιστές και οι testers μπορούν να δημιουργούν αυτοματοποιημένα σενάρια που εκτελούνται επανειλημμένα με συνέπεια, εντοπίζοντας γρήγορα σφάλματα και διασφαλίζοντας τη σωστή λειτουργία του λογισμικού κατά τη διάρκεια των αλλαγών στον κώδικα.

Τα βασικά πλεονεκτήματα της αυτοματοποίησης περιλαμβάνουν:

- Επιτάχυνση της διαδικασίας testing, με αποτέλεσμα την εξοικονόμηση χρόνου σε έργα που περιλαμβάνουν επαναλαμβανόμενες ή εκτεταμένες δοκιμές.
- Δυνατότητα επαναχρησιμοποίησης των σεναρίων δοκιμής (scripts) σε πολλαπλά έργα ή διαφορετικές φάσεις ανάπτυξης, γεγονός που αυξάνει την αποδοτικότητα.
- Ευκολία προσαρμογής των δοκιμών σε διαφορετικά περιβάλλοντα, πλατφόρμες και λειτουργικά συστήματα, κάτι ιδιαίτερα σημαντικό για εφαρμογές που απευθύνονται σε ευρύ κοινό.

Παρόλα αυτά, η αυτοματοποίηση δεν μπορεί να καλύψει κάθε πτυχή της διαδικασίας testing. Υπάρχουν περιπτώσεις όπου η ανθρώπινη κρίση, παρατήρηση και εμπειρία είναι αναντικατάστατες. Ενδεικτικό παράδειγμα αποτελεί το usability testing, δηλαδή η αξιολόγηση της ευχρηστίας και της εμπειρίας χρήστη, όπου απαιτείται κατανόηση της συμπεριφοράς και των αναγκών του τελικού χρήστη – στοιχεία που τα αυτόματα εργαλεία δεν μπορούν να αξιολογήσουν με ακρίβεια.

Επιπλέον, το αρχικό κόστος δημιουργίας και συντήρησης των αυτοματοποιημένων σεναρίων μπορεί να είναι υψηλό, ειδικά σε έργα με περιορισμένο προϋπολογισμό ή μικρή διάρκεια.

Γι’ αυτόν τον λόγο, σε πολλές περιπτώσεις υιοθετείται ένας συνδυασμός αυτοματοποιημένων και χειροκίνητων δοκιμών, ώστε να επιτευχθεί το βέλτιστο αποτέλεσμα όσον αφορά την ποιότητα, την αξιοπιστία και την εμπειρία του χρήστη.

Τεχνητή Νοημοσύνη στο Testing (AI-based Testing)

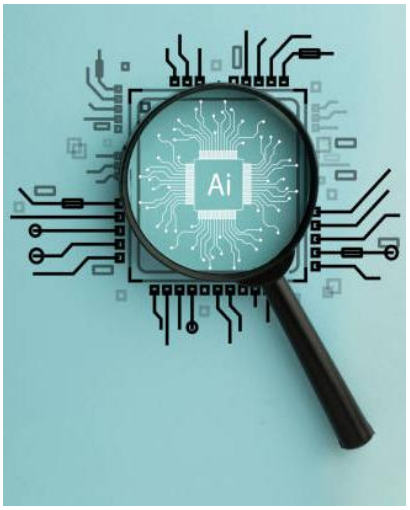
Η τεχνητή νοημοσύνη (AI) εφαρμόζεται όλο και περισσότερο στον τομέα της δοκιμής λογισμικού. (KIRILENKO, 2024) Με τεχνικές machine learning και data analytics, τα εργαλεία AI μπορούν να:

- Δημιουργούν σενάρια δοκιμών αυτόματα.
- Προβλέπουν ποια μέρη του κώδικα είναι πιθανότερο να περιέχουν σφάλματα.
- Βελτιστοποιούν την εκτέλεση δοκιμών ανάλογα με την πιθανότητα αποτυχίας.

Η χρήση AI στο testing υπόσχεται να κάνει τις δοκιμές πιο έξυπνες, στοχευμένες και αποδοτικές.

Continuous Testing σε περιβάλλοντα DevOps

Στο πλαίσιο του DevOps, το Continuous Testing παίζει καθοριστικό ρόλο. (HAMILTON, 2024) Το testing ενσωματώνεται ως αναπόσπαστο κομμάτι της διαδικασίας ανάπτυξης και παράδοσης (Continuous Integration / Continuous Delivery - CI/CD).



Χαρακτηριστικά Continuous Testing:

- Δοκιμή σε κάθε στάδιο του κύκλου ανάπτυξης.
- Άμεση ανατροφοδότηση στους developers.
- Γρήγορη ανίχνευση και διόρθωση σφαλμάτων.
-

Αυτό μειώνει τον κίνδυνο αποτυχιών κατά την παράδοση και επιταχύνει τον χρόνο διάθεσης προϊόντων στην αγορά.

Συμπεράσματα

Το software testing είναι μια πολύπλοκη και πολυδιάστατη διαδικασία που απαιτεί σωστή στρατηγική, μεθοδολογία και εργαλεία για να αποδώσει τα μέγιστα αποτελέσματα. Καμία μέθοδος από μόνη της δεν είναι ικανή να διασφαλίσει την απόλυτη ποιότητα ενός συστήματος.

Η κατανόηση και σωστή εφαρμογή διαφορετικών μεθόδων δοκιμών, όπως το black box, το white box και το gray box testing, σε συνδυασμό με τεχνικές στατικού και δυναμικού testing, εξασφαλίζει την πλήρη κάλυψη των λειτουργικών και μη λειτουργικών απαιτήσεων.

Επιπλέον, η υιοθέτηση σύγχρονων τάσεων όπως η αυτοματοποίηση και η τεχνητή νοημοσύνη επιτρέπει στους οργανισμούς να βελτιώσουν τη διαδικασία δοκιμής, να μειώσουν το χρόνο και το κόστος, και να παραδώσουν προϊόντα υψηλής ποιότητας στους πελάτες.

Συνοψίζοντας, το αποτελεσματικό testing λογισμικού δεν είναι απλώς μια τεχνική ανάγκη, αλλά μια στρατηγική επένδυση στην αξιοπιστία, στην ασφάλεια και στην επιτυχία κάθε πληροφοριακού συστήματος

Αναφορές.

[1]	Grover, P. (2023). Automated Software Testing: Concepts and Techniques. 2nd ed. Springer.
[2]	Hamilton, J. (2024). Modern Testing Tools and Strategies. O'Reilly Media
[3]	BroswerStaRetrievedck.(2025, ΑΠΡΙΛΙΟΣ,5). BroswerStack. Retrieved.from https://www.browserstack.com/guide/what-is-software-testing
[4]	checkpoint. (2025, ΑΠΡΙΛΙΟΣ,13). https://www.checkpoint.com/cyber-hub/cybersecurity/what-is-penetration-testing/what-is-black-box-testing/
[5]	Gobo,K.(2025, ΑΠΡΙΛΙΟΣ,13). Crime. Retrieved from https://www.cprime.com/resources/blog/static-testing-what-you-need-to-know/
[6]	Imperva. (2025). imperv athales company. https://www.imperva.com/learn/application-security/white-box-testing/
[7]	Zaptest. (17 Apr. 2025]. Automated Software Testing Tools and Frameworks. Available at: https://www.zaptest.com

Βιογραφικό συντάκτη.

Ο Ανθχος (Ε) Δημήτριος Γουλόπουλος ΠΝ αποφοίτησε από τη Σχολή Μονίμων Υπαξιωματικών Ναυτικού το 2003 ,με ειδικότητα Ηλεκτρονικός Αυτομάτων Συστημάτων. Έχει ολοκληρώσει όλα τα προβλεπόμενα στο βαθμό του σχολεία και έχει αποφοιτήσει επιτυχώς το 2025 από το Τμήμα Αναλυτών / Προγραμματιστών της Σχολής Προγραμματιστών Ηλεκτρονικών Υπολογιστών του Στρατού Ξηράς.

App Inventor: Ένα εργαλείο για δημιουργική απασχόληση με τις έξυπνες κινητές συσκευές

Μαρία Αλεξάνδρα Ντόντου

Εισαγωγή

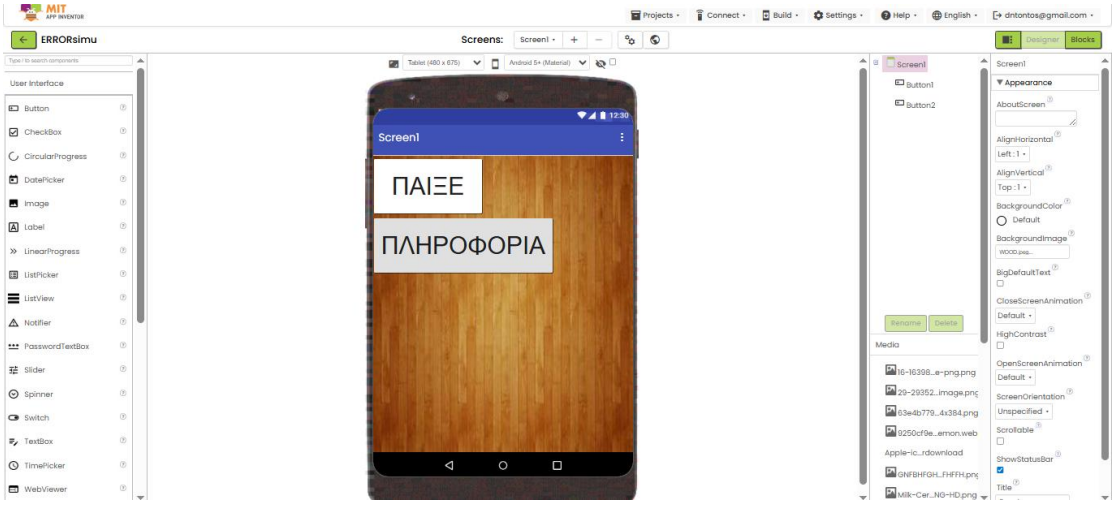
Στον σύγχρονο ψηφιακό κόσμο, η ανάγκη καλλιέργειας υπολογιστικής σκέψης (computational thinking) έχει γίνει ολοένα και πιο επιτακτική. Το MIT App Inventor εμφανίζεται ως μια επαναστατική πλατφόρμα που αποτελεί γέφυρα ανάμεσα στη θεωρητική γνώση και την πρακτική εφαρμογή των αρχών του προγραμματισμού. Η συγκεκριμένη μελέτη εξετάζει τη δομή, τη λειτουργία και τις εκπαιδευτικές δυνατότητες αυτής της πλατφόρμας, με έμφαση στη συμβολή της στην ανάπτυξη κριτικής σκέψης και δημιουργικότητας.

Μικροί και μεγάλοι σπαταλούν μεγάλο μέρος της ημέρας τους χρησιμοποιώντας τις έξυπνες κινητές συσκευές τους. Αν κάποιο από αυτόν τον χρόνο τον αφιέρωναν στην ανάπτυξη εφαρμογών, χρησιμοποιώντας εργαλεία που θα περιόριζαν την απαίτηση για εξειδικευμένες γνώσεις προγραμματισμού, η ενασχόληση με τις συσκευές τους από άσκοπή θα μπορούσε να γίνει εποικοδομητική. Το App Inventor έχει όλα εκείνα τα χαρακτηριστικά για να προσελκύσει το ενδιαφέρον των παιδιών και των νέων και να τους εισάγει στη δημιουργική απασχόληση της ανάπτυξης των δικών τους εφαρμογών.

Δομή και Λειτουργία της Πλατφόρμας

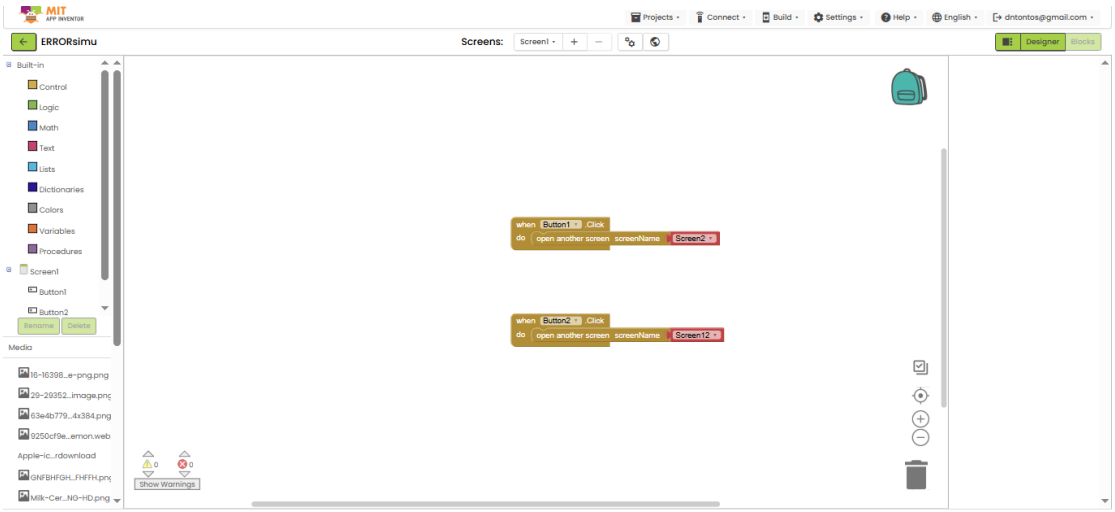
Το MIT App Inventor βασίζεται σε ένα διπλό περιβάλλον εργασίας που απλοποιεί τη διαδικασία ανάπτυξης εφαρμογών. Στο πρώτο επίπεδο, που αναφέρεται ως Designer, ο χρήστης έχει τη δυνατότητα να δημιουργήσει τη διεπαφή της εφαρμογής μέσω ενός γραφικού συστήματος drag-and-drop.

Αυτό το περιβάλλον προσφέρει ένα ευρύ φάσμα στοιχείων διεπαφής χρήστη (UI components), από βασικά κουμπιά έως προηγμένα στοιχεία όπως λίστες και χάρτες.



Εικόνα 7: Ο designer του App Inventor

Το δεύτερο επίπεδο είναι ο Blocks Editor, όπου πραγματοποιείται ο ουσιαστικός προγραμματισμός. Αντί της παραδοσιακής γραφής κώδικα, ο χρήστης συνδέει λογικά blocks που αντιπροσωπεύουν εντολές, συναρτήσεις και δομές ελέγχου. Αυτό το οπτικό σύστημα προγραμματισμού έχει αποδειχτεί ιδιαίτερα αποτελεσματικό στην εκμάθηση βασικών προγραμματιστικών εννοιών, όπως οι δομές επιλογής και επανάληψης, χωρίς την επιβάρυνση της σύνταξης.

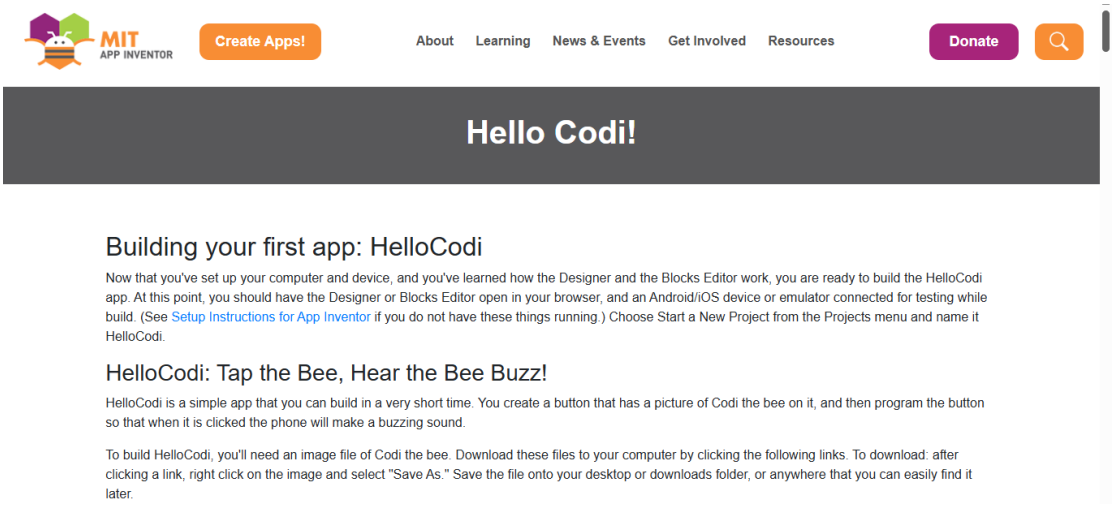


Εικόνα 8: Ο Block Editor του App Inventor

Εκπαιδευτικές Προσεγγίσεις και Δυνατότητες

Η πλατφόρμα ενσωματώνει αρχές κατασκευαστικής μάθησης (constructivist learning), επιτρέποντας στους μαθητές να αναπτύξουν ενεργά τη γνώση τους μέσω πρακτικής εμπειρίας. Έρευνες έχουν δείξει ότι αυτή η προσέγγιση ενισχύει σημαντικά τη κατανόηση αφηρημένων εννοιών και προάγει την ικανότητα επίλυσης προβλημάτων.

Το σύστημα προσφέρει πολλαπλά επίπεδα δυσκολίας, καθιστώντας το κατάλληλο τόσο για αρχάριους όσο και για προχωρημένους χρήστες. Βασικές λειτουργίες όπως η δημιουργία απλών δια δραστικών εφαρμογών μπορούν να αφομοιωθούν σε λίγες ώρες, ενώ οι προηγμένες δυνατότητες (όπως η χρήση αισθητήρων ή η σύνδεση με εξωτερικές βάσεις δεδομένων) απαιτούν βαθύτερη κατανόηση.



Εικόνα 9: Tutorial του App Inventor

Τεχνικές Λεπτομέρειες και Δυναμικότητα

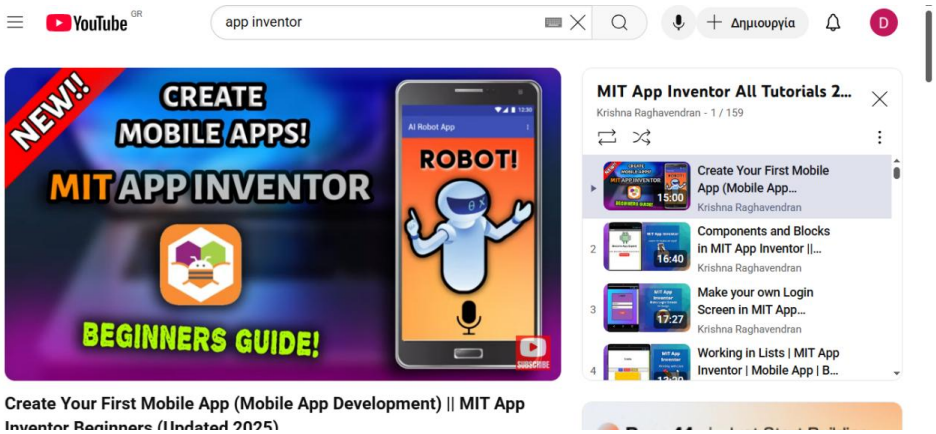
Από τεχνικής άποψης, η πλατφόρμα χρησιμοποιεί μια μεταγλωττισμένη έκδοση του κώδικα σε Blocks, που μετατρέπεται σε Java bytecode για εκτέλεση σε συσκευές Android. Αυτή η αρχιτεκτονική εξασφαλίζει ικανοποιητική απόδοση.

Εκτεταμένες Δυνατότητες και Εκπαιδευτικές Προεκτάσεις

Η πλατφόρμα διακρίνεται για την ευρεία τεχνολογική υποστήριξη που προσφέρει, καθώς και για τις πολυδιάστατες εκπαιδευτικές εφαρμογές της.

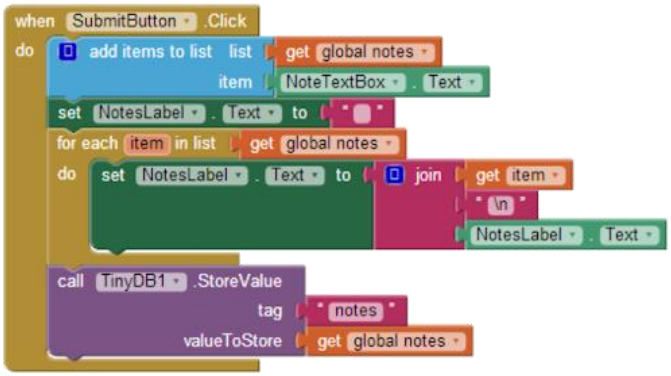
Από τεχνικής πλευράς, το σύστημα παρέχει ολοκληρωμένη πρόσβαση στο υλικό των συσκευών Android, επιτρέποντας την αξιοποίηση ολοκλήρου του φάσματος των αισθητήρων (GPS, επιταχυνσιομέτρου, γυροσκοπίου κ.ά.), καθώς και τη σύνδεση με εξωτερικές υπηρεσίες διαδικτύου μέσω REST APIs.

Η αρχιτεκτονική της πλατφόρμας χαρακτηρίζεται από υψηλή επεκτασιμότητα, υποστηρίζοντας τόσο την εισαγωγή προσαρμοσμένων στοιχείων (custom components) όσο και την άμεση δοκιμή των εφαρμογών σε πραγματικό χρόνο μέσω ασύρματης σύνδεσης.



Εικόνα 10: Σειρά εκπαιδευτικών βίντεο για το App Inventor

Στο εκπαιδευτικό πεδίο, η πλατφόρμα έχει αποδειχτεί ιδιαίτερα αποτελεσματική ως εργαλείο διδασκαλίας βασικών αρχών της πληροφορικής. Συγκεκριμένα, διευκολύνει την εισαγωγή μαθητών στην αλγοριθμική σκέψη μέσω της οπτικής αναπαράστασης προγραμματιστικών δομών, ενώ ταυτόχρονα βοηθά στην κατανόηση αφηρημένων μαθηματικών εννοιών μέσω διαδραστικής οπτικοποίησης. Πέρα από τις τεχνικές δεξιότητες, η χρήση της πλατφόρμας σε ομαδικά έργα συμβάλλει στην ανάπτυξη κρίσιμων διαπροσωπικών ικανοτήτων, όπως η συνεργασία και η επικοινωνία.



Εικόνα 11: Block κώδικα

Επιπλέον, η δυνατότητα δημιουργίας πλήρων λειτουργικών εφαρμογών καλλιεργεί την επιχειρηματική σκέψη, προσφέροντας στους μαθητές την ευκαιρία να μετατρέψουν τις θεωρητικές γνώσεις τους σε απτά και χρήσιμα προϊόντα.

Αυτή η προσέγγιση μετασχηματίζει τη διαδικασία μάθησης από μια παθητική εμπειρία σε μια δυναμική και παραγωγική δραστηριότητα, ενισχύοντας ταυτόχρονα τόσο τις τεχνικές όσο και τις μετα-γνωστικές δεξιότητες των μαθητών. Η ευελιξία και η πολυπλοκότητα του συστήματος το καθιστούν ιδανικό εργαλείο για σύγχρονες εκπαιδευτικές μεθοδολογίες που επιδιώκουν την ολοκληρωμένη ανάπτυξη του μαθητή.

Συμπεράσματα

Το MIT App Inventor αποτελεί ένα ισχυρό εργαλείο για τη σύγχρονη εκπαίδευση, που συνδυάζει την προσβασιμότητα με την εκπαιδευτική αυστηρότητα. Η ικανότητά του να μετατρέπει αφηρημένες έννοιες σε απτές εφαρμογές το καθιστά ιδανικό για την καλλιέργεια υπολογιστικής σκέψης σε όλα τα εκπαιδευτικά επίπεδα. Μελλοντικές έρευνες θα μπορούσαν να εστιάσουν στη μακροπρόθεσμη επίδραση της χρήσης τέτοιων εργαλείων στην ανάπτυξη προγραμματιστικών δεξιοτήτων.

Αναφορές.

[1]	Tony Gaddis, Rebecca Halsey (2015), Starting Out with App Inventor for Android, διαθέσιμο στο https://opac.atmaluhur.ac.id/uploaded_files/temporary/DigitalCollection/MjM5NmFiZWU5MmQwOGE3Mzk1OTg5MzExNGQ0Y2M1ZDc3YWZjYjEwNA==.pdf
[2]	HuiRu Shih (2014), Using MIT App Inventor in an Emergency Management Course to Promote
[3]	Computational Thinking, διαθέσιμο στο https://peer.asee.org/using-mit-app-inventor-in-an-emergency-management-course-to-promote-computational-thinking.pdf
[4]	St. Georgiev, (2019), Students' Viewpoint about Using MIT App Inventor in Education, διαθέσιμο στο https://ieeexplore.ieee.org/document/8756671/authors#authors
[5]	Hal Abelson, Eni Mustafaraj, Franklyn Turbak, Ralph Morelli, Chinma Uche (2012), Lessons learned from teaching App Inventor, διαθέσιμο στο https://dl.acm.org/doi/abs/10.5555/2184451.2184461#core-cited-by
[6]	Benjamin Xie, Hal Abelson (2016), Skill Progression in MIT App Inventor, διαθέσιμο στο https://www.benjixie.com/publication/vlhcc-2016/vlhcc-2016.pdf

Βιογραφικό συντάκτη.

Η Μαρία-Αλεξάνδρα Ντόντου είναι φοιτήτρια του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Ιωαννίνων. όπου διανύει ήδη το τέταρτο έτος των σπουδών της. Την τρέχουσα χρονική περίοδο συντάσσει τη διπλωματική εργασία με τίτλο "Βελτιστοποίηση προπόνησης και πρόβλεψη επιδόσεων στην αγωνιστική κολύμβηση με τεχνικές μηχανικής μάθησης και όρασης".

Κατέχει επίσης δίπλωμα ναυαγοσώστη και είναι εν ενεργεία αθλήτρια της κλασικής κολύμβησης, με συμμετοχές και διακρίσεις σε εθνικά πρωταθλήματα και αγωνιστικές ημερίδες.

ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ.

- **Επίσκεψη της 144ης και 145ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος**

Στις 23 Ιαν 25 πραγματοποιήθηκε επίσκεψη στις εγκαταστάσεις της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, με τη συμμετοχή του συνόλου των σπουδαστών της 144ης και 145ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών της ΣΠΗΥ, (18 άτομα). Οι σπουδαστές της Σχολής ενημερώθηκαν για την αποστολή, το έργο και τις δράσεις της Διεύθυνσης. Επίσης, τους δόθηκε η δυνατότητα να διαπιστώσουν, το πως εφαρμόζονται στην πράξη, αντικείμενα που περιλαμβάνονται στην εκπαίδευση τους.

- **Συμμετοχή της 145ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών στο 1ο Cyber Intelligence Forum**

Η ΣΠΗΥ συμμετείχε στο 1ο Cyber Intelligence Forum, που πραγματοποιήθηκε στις 04 Φεβ 2025 στο Μέγαρο Μουσικής Αθηνών, με οκτώ σπουδαστές της 145ης ΕΣ του Τμήματος Αναλυτών – Προγραμματιστών. Οι εισηγήσεις και οι συζητήσεις, περιλαμβάναν εκτενείς αναφορές σε αναδυόμενες ψηφιακές απειλές, αμυντικούς μηχανισμού, εργαλεία και τεχνικές για τον εντοπισμό και τον περιορισμό των ευπαθειών σε πραγματικό χρόνο.

- **Επίσκεψη της 144ης και 145ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών στο Τμήμα Προσομοίωσης ΓΕΕΘΑ/Α3/4.**

Στο πλαίσιο προγραμματισμένων επισκέψεων, στις 14 Φεβ 25 πραγματοποιήθηκε επίσκεψη με το σύνολο των σπουδαστών της 144ης και 145ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών της ΣΠΗΥ (18 άτομα), στο Τμήμα Προσομοίωσης ΓΕΕΘΑ/Α3/4. Οι σπουδαστές ενημερώθηκαν για τις δραστηριότητες του Τμήματος και για τεχνικά στοιχεία ανάπτυξης προσομοιώσεων.

- **Αποφοίτηση Σχολείου Διαχειριστών Πληροφοριακών Συστημάτων (Α΄ ΕΣ 2025).**

Στις 21 Φεβ 25, πραγματοποιήθηκε στην έδρα της Σχολής, η τελετή αποφοίτησης του Σχολείου Διαχειριστών Πληροφοριακών Συστημάτων (Α΄ ΕΣ 2025). Αποφοίτησαν συνολικά είκοσι τέσσερα (24) άτομα. Δεκατρία (13) στελέχη του ΣΞ, τρία (3) του ΠΝ, ένας (1) της ΠΑ, πέντε (5) του ΓΕΕΘΑ, ένας (1) του ΛΣ ΕΛ-ΑΚΤ, και ένας (1) Πολιτικός Υπάλληλος.

- **Αποφοίτηση της 144ης Εκπαιδευτικής Σειράς Αξιωματικών Αναλυτών-Προγραμματιστών**

Στις 21 Φεβρουαρίου 2025 πραγματοποιήθηκε στη ΛΑΕΔ, η αποφοίτηση της 144ης Εκπαιδευτικής Σειράς Αξκών Αναλυτών-Προγραμματιστών της ΣΠΗΥ, παρουσία του Δντή του ΓΕΣ/ΔΙΠΛΗ Συνταγματάρχη (ΠΛΗ) Γεωργίου Χόντου και του Διευθυντή του ΚΕΠΥΕΣ Συνταγματάρχη (ΠΛΗ) Αντωνίου Κόγια. Αποφοίτησαν συνολικά δέκα (10) άτομα. Επτά (7) στελέχη του ΣΞ, δύο (2) του ΠΝ, και ένας (1) του ΠΣ από το ΓΕΕΘΑ. Την τελετή αποφοίτησης τίμησαν με την παρουσία τους ο πρώην Δντής ΓΕΣ/ΔΕΠΛΗ, Αντγος ε.α. κ. Σταυρόπουλος Γαβριήλ και ο πρώην Δκτής της ΣΠΗΥ, Ταξχος ε.α. κ. Κολαΐτης Χρήστος-Χαράλαμπος. Κατά τη διάρκεια της τελετής απονεμήθηκαν αναμνηστικές πλακέτες από τον Δκτή της ΣΠΗΥ, Συνταγματάρχη (ΠΛΗ) Δημήτριο Ντόντο, στον Αντισυνταγματάρχη (εα) Ξενοφώντα Κατσιμαγκλή προς αναγνώριση της πολυετούς πολύτιμης συνεισφοράς του στο εκπαιδευτικό έργο της Σχολής, καθώς και στα τέκνα των επιτελών της ΣΠΗΥ για την εισαγωγή τους στην ανώτατη εκπαιδευτική βαθμίδα.

- **Ολοκλήρωση Επιμορφωτικών Προγραμμάτων Η/Υ ΔΙΜΑ, για το Πολιτικό Προσωπικό του ΥΠΕΘΑ**

Στις 04 Απρ 25 ολοκληρώθηκαν τα Επιμορφωτικά Προγράμματα Η/Υ ΔΙΜΑ, «Χειρισμός Ηλεκτρονικών Υπολογιστών και Διαχείρισης Αρχείων, Περιήγησης στο Διαδίκτυο, Χρήσης Ηλεκτρονικού Ταχυδρομείου» και «Βασικό Επίπεδο Γνώσεων Επεξεργασίας Κειμένων Word Ι». Η διάρκεια των εκπαιδευτικών προγραμμάτων ήταν μία εβδομάδα έκαστο και συμμετείχαν συνολικά σαράντα ένα (41) Μόνιμοι Πολιτικοί Υπάλληλοι.

- **Τελετή αποφοίτησης 6ου Βασικού Σχολείου Πληροφορικής**

Στις 04 Απριλίου 2025, πραγματοποιήθηκε στη ΛΑΕΔ, η τελετή αποφοίτησης του 6ου Βασικού Σχολείου Πληροφορικής της ΣΠΗΥ παρουσία του Διευθυντή του ΓΕΕΘΑ/Β8, Υποστράτηγου (ΠΛΗ) Χατζηδάκη Εμμανουήλ, ο οποίος απένειμε τα πτυχία. Στο πλαίσιο της τελετής, τιμήθηκε με αναμνηστική πλακέτα, από το Δκτή της ΣΠΗΥ, Συνταγματάρχη (ΠΛΗ) Ντόντο Δημήτριο, ο Αντιστράτηγος ε.α. κ. Φραγκουλόπουλος Εμμανουήλ, προς αναγνώριση της πολυετούς συνεισφοράς του στην αξιοποίηση των εφαρμογών πληροφορικής στις ΕΔ.

- **Ολοκλήρωση Σχολείου Ασφαλείας Πληροφοριακών Συστημάτων & Δικτύων Η/Υ (Α΄ ΕΣ 2025)**

Το χρονικό διάστημα από 05/05/25 – 13/06/25 διεξήχθη στις εγκαταστάσεις της ΣΠΗΥ, το Σχολείο Ασφαλείας Πληροφοριακών Συστημάτων και Δικτύων Η/Υ (Α΄ ΕΣ 2025).

Αποφοίτησαν συνολικά δέκα εννέα (19) άτομα. Τέσσερα (4) στελέχη του ΓΕΕΘΑ, δέκα τρία (13) στελέχη του ΣΞ, ένα (1) στέλεχος του ΠΝ, και ένα (1) στέλεχος του ΓΕΑ.

.

- **Σεμινάριο Ναυαγοσωστικής και πρώτων βοηθειών**

Στις 25 Ιουνίου 2025, στο πλαίσιο ανακήρυξης του έτους 2025 από το ΓΕΣ, ως «έτος αφιερωμένο στην αναγνώριση του ρόλου και στην απόδοση τιμής, στις οικογένειες του στρατιωτικού προσωπικού», πραγματοποιήθηκε στις εγκαταστάσεις της ΣΠΗΥ, σεμινάριο με θέμα «Ναυαγοσωστική και Πρώτες Βοήθειες» με την συμμετοχή είκοσι (20) ατόμων από το μόνιμο προσωπικό και τους εκπαιδευόμενους της Σχολής. Εισηγήτρια ήταν η Μαρία-Αλεξάνδρα Ντόντου, πτυχιούχος Ναυαγοσώστης και αθλήτρια της κλασικής κολύμβησης με συμμετοχές και διακρίσεις.

- **Παρουσίαση Πτυχιακών Εργασιών της 145ης Εκπαιδευτικής Σειράς Αξιωματικών Αναλυτών-Προγραμματιστών**

Στις 25 Ιουνίου 2025 πραγματοποιήθηκε στην έδρα της ΣΠΗΥ, η παρουσίαση των πτυχιακών εργασιών της 145ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών παρουσία του Δντή του ΓΕΣ/ΔΙΠΛΗ, Συνταγματάρχη (ΠΛΗ) Ιωάννη Λιώτα, του Δκτή της ΣΠΗΥ Συνταγματάρχη (ΠΛΗ) Δημητρίου Ντόντου, καθώς και εκπροσώπων του ΓΕΝ/Β2, του ΚΕΠΥΕΣ και καθηγητών της Σχολής. Οι εργασίες αφορούσαν: την ανάπτυξη και εφαρμογή ενός Ψηφιακού Διδύμου (Digital Twin) αξονικού συστήματος πλοίου και την ενσωμάτωση Ψηφιακού Βοηθού (chatbot) στο σύστημα του ΗΚΕΛΥ, βασισμένου σε τεχνολογίες μηχανικής μάθησης.

- **Αποφοίτηση της 145ης Εκπαιδευτικής Σειράς Αξιωματικών Αναλυτών-Προγραμματιστών**

Στις 27 Ιουνίου 2025 πραγματοποιήθηκε στη ΛΑΕΔ, η αποφοίτηση της 145ης Εκπαιδευτικής Σειράς Αξκών Αναλυτών-Προγραμματιστών της ΣΠΗΥ, παρουσία του Δντή του ΓΕΕΘΑ/Β8 Υποστράτηγου (ΠΛΗ) Χατζηδάκη Βασιλείου, ο οποίος απένειμε τα πτυχία στους αποφοιτήσαντες. Αποφοίτησαν συνολικά οκτώ () άτομα. Πέντε (5) στελέχη στου ΣΞ, δύο (2) του ΠΝ και ένας (1) του ΝΟΜ από το ΓΕΕΘΑ. Την τελετή αποφοίτησης τίμησαν με την παρουσία τους ο πρώην Δντής ΓΕΣ/ΔΕΠΛΗ, Αντγος (ε.α). κ. Σταυρόπουλος Γαβριήλ, εκπρόσωποι του ΓΕΕΘΑ/Α3/4, του ΚΕΠΥΕΣ, του ΓΕΝ/Α4, του ΓΕΝ/Β2 και καθηγητές της σχολής. Κατά τη διάρκεια της τελετής απονεμήθηκαν αναμνηστικές πλακέτες από τον Δκτή της ΣΠΗΥ, Συνταγματάρχη (ΠΛΗ) Δημήτριο Ντόντο, στους: Σχη (ΠΛΗ) Καλοφύρη Αθανάσιο, Σχη (ΠΛΗ) Τσεσμετζή Παναγιώτη, Ανχη (ΠΛΗ) Τσιούγκο Χρυσοβαλάντη, Ανχη (ΠΛΗ) Τρίκκα Αθανάσιο και Ανχη (ΠΛΗ) Σαρρή Παναγιώτη, προς αναγνώριση της πολυετούς πολύτιμης συνεισφοράς τους στο εκπαιδευτικό έργο της Σχολής.

- **Ολοκλήρωση Επιμορφωτικών Προγραμμάτων Η/Υ Φυσικής παρουσίας (ΦΠ) & Διαδικτυακής Μάθησης (ΔΙΜΑ), για το Πολιτικό Προσωπικό του ΥΠΕΘΑ**

Στις 03 Οκτ 25 ολοκληρώθηκε το Επιμορφωτικό Πρόγραμμα Η/Υ «Βασικών Δεξιοτήτων Βάσεων Δεδομένων Access» με Φυσική Παρουσία στις εγκαταστάσεις της Σχολής και ΔΙΜΑ. Η διάρκεια του εκπαιδευτικού προγράμματος ήταν μία εβδομάδα και

συμμετείχαν συνολικά είκοσι τρείς (23) Μόνιμοι Πολιτικοί Υπάλληλοι, έντεκα (11) με δια ζώσης εκπαίδευση και δώδεκα (12) μέσω ΔΙΜΑ.

Στις 24 Οκτ 25 ολοκληρώθηκε το Επιμορφωτικό Πρόγραμμα Η/Υ «Προχωρημένο Επίπεδο Υπολογιστικών Φύλλων Excel ΙΙ» μέσω ΔΙΜΑ. Η διάρκεια του εκπαιδευτικού προγράμματος ήταν μία εβδομάδα και συμμετείχαν συνολικά δέκα επτά (17) Μόνιμοι Πολιτικοί Υπάλληλοι.

- **Αποφοίτηση Σχολείου Διαχειριστών Πληροφοριακών Συστημάτων (Β΄ ΕΣ 2025).**

Στις 10 Οκτ 25, πραγματοποιήθηκε στην έδρα της Σχολής, η τελετή αποφοίτησης του Σχολείου Διαχειριστών Πληροφοριακών Συστημάτων (Β΄ ΕΣ 2025). Αποφοίτησαν συνολικά δέκα τρία (13) άτομα. Οκτώ (8) στελέχη του ΣΞ, τρία (3) του ΠΝ και δύο (2) στελέχη του ΓΕΕΦ.

- **Ολοκλήρωση Σχολείου Ασφαλείας Πληροφοριακών Συστημάτων & Δικτύων Η/Υ (Β΄ ΕΣ 2025)**

Το χρονικό διάστημα από 13 Οκτ 25 έως 21 Νοε 25 διεξήχθη στις εγκαταστάσεις της ΣΠΗΥ, το Σχολείο Ασφαλείας Πληροφοριακών Συστημάτων και Δικτύων Η/Υ (Β΄ ΕΣ 2025). Αποφοίτησαν συνολικά δέκα εννέα (19) άτομα. Τέσσερα (4) στελέχη του ΓΕΕΘΑ, δέκα τρία (13) στελέχη του ΣΞ, ένα (1) στέλεχος του ΓΕΕΦ και ένα (1) στέλεχος της ΕΛΑΣ.

- **Συμμετοχή των σπουδαστών της 146ης Εκπαιδευτικής Σειράς Προγραμματιστών στο 10ο Συνέδριο «DPO & ICT Security World/ e-Government Forum 2025»**

Η ΣΠΗΥ συμμετείχε στο 10ο συνέδριο «Data Protection Officer & Information Communication Technology» στο πλαίσιο του 15ου ετήσιου «e-Government Forum», που πραγματοποιήθηκε την Τετάρτη 26 Νοεμβρίου 2025 στο Ωδείο Αθηνών, με 10 σπουδαστές της 146ης ΕΣ του Τμήματος Προγραμματιστών και συνοδεία στελεχών του ΚΔΒΜ της Σχολής. Το συνέδριο είχε ως επίκεντρο τη Ψηφιακή Ασφάλεια, την προστασία προσωπικών δεδομένων και τις νέες προκλήσεις της τεχνητής νοημοσύνης (ΤΝ) στο δημόσιο και ιδιωτικό τομέα. Οι εισηγήσεις και οι συζητήσεις, περιλαμβάναν εκτενείς αναφορές σε αναδυόμενες ψηφιακές απειλές, αμυντικούς μηχανισμούς, εργαλεία και τεχνικές για τον εντοπισμό και τον περιορισμό των ευπαθειών σε πραγματικό χρόνο. Το συνέδριο πραγματοποιήθηκε υπό την αιγίδα του Υπουργείου Ψηφιακής Διακυβέρνησης (ΥΨΗΔ) και της ΗΔΙΚΑ Α.Ε..

Όροι Συνεργασίας

Σκοπός

Το περιοδικό «ΗΛΕΚΤΡΟΝΙΟ» εκδίδεται από τη ΣΠΗΥ κάθε εξάμηνο με σκοπό την προώθηση πληροφοριών σχετικά με τις εξελίξεις στο χώρο της πληροφορικής και τις εφαρμογές της.

Η θεματολογία του περιοδικού περιλαμβάνει κείμενα σχετικά με:

- επιστημονικές εργασίες.
- εφαρμογές της πληροφορικής.
- νέες μεθοδολογίες και τεχνικές.
- την ιστορική εξέλιξη της πληροφορικής.
- τις δραστηριότητες της Σχολής.

Τα κείμενα που δημοσιεύονται εκφράζουν τον συντάκτη και δεν απηχούν απαραίτητα τις απόψεις της Σχολής.

Τα προς δημοσίευση άρθρα θα πρέπει να πληρούν τους παρακάτω κανόνες:

- Τα κείμενα δεν θα πρέπει να υπερβαίνουν τις 5.000 λέξεις. Επιπλέον θα πρέπει να περιλαμβάνουν επαρκή τεκμηρίωση και βιβλιογραφία.
- Η υποβολή των κειμένων θα πρέπει να γίνεται σε ηλεκτρονική επεξεργάσιμη μορφή στη διεύθυνση ηλεκτρονικού ταχυδρομείου **sphy_3@army.gr**.
- Οι συντάκτες των άρθρων θα πρέπει να υποβάλλουν και ένα σύντομο βιογραφικό (με φωτογραφία προαιρετικά) το οποίο θα προστίθεται στο τέλος του κειμένου.
- Τα κείμενα απαγορεύονται διαβαθμισμένες πληροφορίες.

ΣΠΗΥ
17 Δεκ 2025