Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Η Διδασκαλία της Κυβερνοασφάλειας στη Μέση Τεχνική Εκπαίδευση

Άντρη Χριστοφή

Επιβλέπουσα Καθηγήτρια
Αδαμαντίνη Περατικού

Νοέμβριος 2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Η Διδασκαλία της Κυβερνοασφάλειας στη Μέση Τεχνική Εκπαίδευση

Άντρη Χριστοφή

Επιβλέπουσα Καθηγήτρια
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Νοέμβριος 2022

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Εισαγωγή: Παρά το γεγονός ότι το Διαδίκτυο έχει επηρεάσει θετικά τις ζωές των ανθρώπων, προέκυψαν αρνητικά ζητήματα που σχετίζονται με τη χρήση του Διαδικτύου. Περιπτώσεις όπως ο διαδικτυακός εκφοβισμός, η διαδικτυακή απάτη, η ρατσιστική κακοποίηση, η πορνογραφία και ο τζόγος είχαν αυξηθεί πάρα πολύ λόγω της έλλειψης συνειδητοποίησης και αυτο-μηχανισμού μεταξύ των χρηστών του Διαδικτύου για να προστατευθούν από το να πέσουν θύματα αυτών των πράξεων. Ένα από τα ζωτικά μέτρα που πρέπει να ληφθούν είναι η καλλιέργεια της γνώσης και της ευαισθητοποίησης μεταξύ των χρηστών του Διαδικτύου από την πρώιμη ηλικία τους, δηλαδή των παιδιών. Τα παιδιά, συγκεκριμένα, είναι σημαντικό να εκπαιδεύονται ώστε να λειτουργούν με ασφαλή τρόπο στον κυβερνοχώρο και να προστατεύονται στη διαδικασία.

Σκοπός: Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι η διεξοδική μελέτη των στάσεων και των απόψεων των εκπαιδευτικών μηχανικής υπολογιστών και ηλεκτρολογίας των Τεχνικών Σχολών της Κύπρου σχετικά με τη διδασκαλία της κυβερνοασφάλειας στα σχολεία.

Μέθοδος: Η μέθοδος έχει χρησιμοποιηθεί είναι αυτή της ποσοτικής έρευνας. Το μέσο συλλογής δεδομένων της έρευνας ήταν το ερωτηματολόγιο, το οποίο δόθηκε ηλεκτρονικά στα σχολεία Μέσης Τεχνικής Εκπαίδευσης της Κύπρου. Το δείγμα της έρευνας αποτελειτο από 100 εκπαιδευτικούς μηχανικής υπολογιστών και ηλεκτρολογίας. Τα δεδομένα της έρευνας αυτής κωδικοποιήθηκαν και αναλύθηκαν με το στατιστικό πρόγραμμα SPSS. Τα αποτελέσματα της έρευνας αυτής συγκρίθηκαν και με άλλες όμοιες έρευνες που έχουν γίνει σε Ελλάδα και εξωτερικό.

Αποτελέσματα: Τα αποτελέσματα της έρευνας αυτής έχουν δείξει ότι γενικά υπάρχει μια θετική στάση των εκπαιδευτικών για να διδάξουν το μάθημα ασφάλειας στον κυβερνοχώρο, παρόλα αυτά θεωρούν ότι θα υπάρχουν προβλήματα από την εφαρμογή αυτή λόγω του ότι είναι κάτι καινούργιο.

Συμπεράσματα: Συνεπώς, μέσα από τα αποτελέσματα της έρευνας αυτής έχει φανεί ότι οι εκπαιδευτικοί της Μέσης Τεχνικής Εκπαίδευσης της Κύπρου θα ήθελαν να διδάξουν το μάθημα της ασφάλειας στον Κυβερνοχώρο στις Τεχνικές Σχολές της Κύπρου. Παρόλα αυτά θα χρειάζονταν επιμόρφωση για να γίνει αυτό. Είναι σημαντικό να γίνει μια μεγαλύτερη έρευνα με ακόμα μεγαλύτερο δείγμα ώστε να παρουσιαστούν οι στάσεις των εκπαιδευτικών όλων των βαθμίδων της Κύπρου για τη διδασκαλία της κυβερνοασφάλειας στα σχολεία.

Abstract

Introduction: Even though the Internet has positively affected people's lives, negative issues have arisen related to the use of the Internet. Cases such as cyberbullying, online fraud, racial abuse, pornography, and gambling had increased tremendously due to the lack of awareness and self-mechanism among internet users to protect themselves from falling victim to these acts. One of the vital measures to be taken is to cultivate knowledge and awareness among Internet users from their early age, namely children. It is important for children to be educated to operate in a safe manner in cyberspace and protect themselves in the process.

Purpose: The purpose of this master's thesis is the thorough study of the attitudes and opinions of computer engineering and electrical engineering teachers at the Technical Schools of Cyprus regarding the teaching of cyber security in schools.

Method: The method used is that of quantitative research. The means of data collection of the research was the questionnaire, which was given electronically to the Secondary Technical Education schools of Cyprus. The research sample consisted of 100 computer and electrical engineering teachers. The data of this research were coded and analyzed with the SPSS statistical program. The results of this research were compared with other similar researches that have been done in Greece and abroad.

Results: The results of this research have shown that in general there is a positive attitude of the teachers to teach the cyber security course, however they think that there will be problems from this implementation due to the fact that it is something new.

Conclusions: Therefore, through the results of this research it has been seen that the teachers of the Secondary Technical Education of Cyprus would like to teach the subject of cyber security in the Technical Schools of Cyprus. However, they would need training to do this. It is important to conduct a larger survey with an even larger sample in order to present the attitudes of teachers of all levels in Cyprus regarding the teaching of cyber security in schools.

Ευχαριστίες

Και τελικά ήρθε η στιγμή που πάρα πολύ περίμενα. Την περίμενα με όλη μου την ψυχή! Η παράδοση της δικής μου διατριβής… Ευχαριστώ! Ευχαριστώ το Θεό που με αξίωσε να φτάσω σε αυτό το σημείο! Τον ευχαριστώ για τη δύναμη που μου έδωσε! Ευχαριστώ την οικογένειά μου και ιδιαίτερα το σύζυγο μου, που χωρίς αυτόν δεν θα κατάφερνα να ολοκληρώσω τις σπουδές μου στο Ανοικτό Πανεπιστήμιο Κύπρου. Βέβαια, θα ήταν παράληψή μου να μην ευχαριστήσω την καθηγήτριά μου κα Αδαμαντίνη Περατικού για την πολύτιμη καθοδήγηση. Αφιερώνω αυτή τη διατριβή στις κόρες μου, Παναγιώτα και Ιωάννα.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η ασφάλεια στον κυβερνοχώρο διαδραματίζει σημαντικό ρόλο στη σημερινή κοινωνία, φτάνοντας σε παγκόσμια δαπάνη 145 δισεκατομμυρίων δολαρίων κατά το έτος 2018 [1]. Τα σχέδια για βελτίωση της ασφάλειας στον κυβερνοχώρο αποτελούν το επίκεντρο πολλών κυβερνήσεων. Υπάρχει ανάγκη για να καλυφθεί το χάσμα δεξιοτήτων και εργατικού δυναμικού και να βελτιωθεί ο αλφαβητισμός στον κυβερνοχώρο. Η υιοθέτηση της τεχνολογίας στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση βρίσκεται σε συνεχή ανάπτυξη καθώς οι εκπαιδευτικοί προετοιμάζουν τους μαθητές για τη ζωή και την καριέρα τους μετά την εκπαίδευση και υιοθετούν γρήγορα νέες και αναδυόμενες τεχνολογίες για να βοηθήσουν στην παροχή διδασκαλίας και μάθησης, διοικητικών καθηκόντων και κοινοτικής συμμετοχής. Ο ρόλος της ασφάλειας στον κυβερνοχώρο στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση είναι να ενισχύσει τη συνολική στάση ασφάλειας του κλάδου, ενώ ταυτόχρονα δεν εμποδίζει την παροχή παιδαγωγικής, διδασκαλίας και μάθησης, διοικητικών καθηκόντων και κοινοτικής συμμετοχής [2].

Τα πρωτοβάθμια και δευτεροβάθμια εκπαιδευτικά ιδρύματα είναι πρωταρχικοί στόχοι για κυβερνοεπιθέσεις. Αποτελούν επίσης ένα μοναδικό περιβάλλον όπου το μεγαλύτερο μέρος της χρήσης γίνεται από παιδιά, ακολουθούμενο από διδακτικό προσωπικό και διοικητικό προσωπικό. Αυτό εισάγει μοναδικές προκλήσεις κατά την εφαρμογή πλαισίων ασφάλειας στον κυβερνοχώρο που εισάγουν ελέγχους και πολυπλοκότητες, καθώς απαιτούν υιοθέτηση, αλληλεπίδραση, κατανόηση και ευαισθητοποίηση των χρηστών, τους ανθρώπινους παράγοντες. Παραδείγματα είναι η χρήση διαδικτυακών εργαλείων και πόρων [3], καθώς και η υιοθέτηση εξ αποστάσεως μάθησης [4] και της εξ αποστάσεως εκπαίδευσης. Επιπλέον, η υιοθέτηση διαδικτυακών εργαλείων αυξήθηκε με το κλείσιμο σχολείων κατά τη διάρκεια της πανδημίας του Covid-19 [5], αυξάνοντας την έκθεση του προσωπικού και των μαθητών σε κινδύνους για την ασφάλεια στον κυβερνοχώρο, καθώς οι δραστηριότητες άρχισαν να διεξάγονται στο Διαδίκτυο.

Ο στόχος της εκπαίδευσης για την ασφάλεια στον κυβερνοχώρο είναι να εκπαιδεύσει τους χρήστες της τεχνολογίας σχετικά με τους πιθανούς κινδύνους που αντιμετωπίζουν

όταν χρησιμοποιούν εργαλεία επικοινωνίας στο Διαδίκτυο, όπως μέσα κοινωνικής δικτύωσης, συνομιλία, διαδικτυακά παιχνίδια, email και άμεσα μηνύματα. Παρόλο που έχουν διεξαχθεί πολλές έρευνες στο παρελθόν σχετικά με την ασφάλεια στον κυβερνοχώρο, σε διαφορετικούς τομείς, για παράδειγμα οι έρευνες των Kruse [6], Dong [7], Herrera et al. [8], ήταν λίγες εκείνες οι οποίες επικεντρώθηκαν στα βήματα που πρέπει να γίνουν ιδιαίτερα από τα σχολεία προκειμένου να βοηθήσουν στην καλλιέργεια ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο. Ο στόχος αυτής της εργασίας είναι να συζητήσει τις στάσεις και τις θέσεις των εκπαιδευτικών λόγω του ότι είναι κρίσιμο να εκπαιδεύονται οι σύγχρονοι μαθητές σχετικά με τους κινδύνους που συνδέονται με την δραστηριοποίηση στον κυβερνοχώρο.

1.1 Περιγραφή Προβλήματος

Το έγκλημα στον κυβερνοχώρο κατά των παιδιών και των εφήβων είναι σίγουρα ανησυχητικό για τους γονείς. Μερικές φορές δεν συνειδητοποιούν ότι το παιδί τους είναι θύμα ηλεκτρονικού εγκλήματος. Πολλοί γονείς δεν γνωρίζουν τις δραστηριότητες των παιδιών τους στον κυβερνοχώρο [6]. Μερικά παιδιά εκφοβίζονται μέσω σχολίων και προσβολών. Μπορεί επίσης να υποστούν εκφοβισμό, παρενόχληση, κακοποίηση ή ακόμα και σεξουαλική εκμετάλλευση. Αυτή η εργασία πραγματοποιήθηκε με σκοπό να διδαχθούν τα παιδιά την κυβερνοασφάλεια έτσι ώστε να μην γίνουν θύματα διαδικτυακών επιθέσεων.

Όσον αφορά τις προσπάθειες των γονέων να προστατεύσουν τα παιδιά τους από απειλές στον κυβερνοχώρο, δεν υπάρχει αμφιβολία ότι τα παιδιά, παρά το νεαρό της ηλικίας τους, είναι ικανά να χρησιμοποιούν τα δικά τους smartphone. Τα παιδιά δεν είναι μόνο γνώστες της τεχνολογίας, αλλά και ικανά στη χρήση της τεχνολογίας. Μάλιστα, υπάρχουν και γονείς που δίνουν gadget στα παιδιά τους ως επιβράβευση για την αριστεία σε εξετάσεις, δώρα γενεθλίων κ.λπ. Αυτό καθιστά τα παιδιά ευάλωτα στην κακοποίηση μέσω της τεχνολογίας, ενώ εξερευνούν ανεξάρτητα το διαδίκτυο χωρίς όρια ή παρακολούθηση. Επομένως, όταν απολαμβάνονται τα οφέλη του διαδικτύου, είναι σημαντικό για όλους, είτε γονείς είτε παιδιά, να γνωρίζουν πιθανούς κινδύνους όπως ο διαδικτυακός εκφοβισμός, καθώς και να λαμβάνουν προφυλάξεις ασφαλείας, καθώς τα παιδιά έχουν πλέον πρόσβαση στο διαδίκτυο σε μικρότερη ηλικία [7]. Επομένως, το πρόβλημα που καλούνται οι εκπαιδευτικοί να επιλύσουν, είναι να διαδίδουν μηνύματα κυβερνοασφάλειας προκειμένου να προωθήσουν την υπεύθυνη διαδικτυακή συμπεριφορά.

1.2 Σκοπός και Στόχοι

Η παρούσα διατριβή στοχεύει στη διεξοδική μελέτη των στάσεων και των απόψεων των εκπαιδευτικών Μηχανικής Ηλεκτρονικών Υπολογιστών και Ηλεκτρολογίας των Τεχνικών Σχολών της Κύπρου σχετικά με τη διδασκαλία της κυβερνοασφάλειας στα σχολεία.

Τα ερευνητικά ερωτήματα της παρούσας μελέτης είναι τα ακόλουθα:
Ε1: Ποια η στάση των εκπαιδευτικών ως προς την διδασκαλία της κυβερνοασφάλειας στα σχολεία;
Ε2: Ποιες οι απόψεις των εκπαιδευτικών αναφορικά με τη διδασκαλία της κυβερνοασφάλειας στα σχολεία;
Ε3: Με ποιους τρόπους μπορεί να προσφερθεί το μάθημα αυτό στην Μέση Τεχνική Εκπαίδευση;
Ε4: Πως μπορεί το μάθημα αυτό να προσαρμοστεί στις ανάγκες του κάθε εκπαιδευόμενου;

Κεφάλαιο 2
Ανασκόπηση Βιβλιογραφίας

2.1 Εισαγωγή

Στις μέρες μας, η εμφάνιση και η πρόοδος της τεχνολογίας επιτρέπουν στους ανθρώπους να απολαμβάνουν τόσο τον εικονικό κόσμο όσο και τον πραγματικό κόσμο. Για παράδειγμα, οι άνθρωποι είναι γνωστό ότι δημιουργούν ψεύτικες αναρτήσεις στο Instagram και στο Facebook που δείχνουν πλούσιο τρόπο ζωής ενώ ζουν σε συνθήκες φτώχειας. Με εφαρμογές και μηχανές αναζήτησης όπως το YouTube, το Yahoo και η Google, οι ζωτικής σημασίας πληροφορίες είναι πλέον άμεσα διαθέσιμες και προσβάσιμες από όλα τα άτομα με ηλεκτρονικά gadget, όπως υπολογιστές και τηλέφωνα, όπου οι χρήστες μπορούν να χειριστούν το μήνυμα για να επιτύχουν τον στόχο τους ή να δελεάσουν τα θύματά τους [11]. Επίσης, η φυσική αγορά αντικαθίσταται σιγά σιγά από την εικονική αγορά μέσω του ηλεκτρονικού εμπορίου, η οποία αποδεικνύεται μια πιο αποτελεσματική και οικονομικά αποδοτική προσέγγιση για τη λειτουργού των σημερινών επιχειρήσεων. Ανάλογα με την πολιτική του ιστότοπου, ο αγοραστής προσδιορίζει το αντικείμενο που σκοπεύει να αγοράσει, μετά το οποίο πληρώνει πριν ή μετά την παράδοση.

Παρόλα αυτά, οι διαδικτυακές επιχειρήσεις έχουν συμβάλει δραματικά σε διαδικτυακές απάτες και εγκλήματα στον κυβερνοχώρο. Για παράδειγμα, ένας αγοραστής μπορεί να αγοράσει ένα αντικείμενο που δεν υπάρχει αλλά εμφανίζεται σε μια διαδικτυακή αγορά και ως εκ τούτου, ο αγοραστής συχνά εξαπατάται [12]. Σε άλλες περιπτώσεις, ο αγοραστής μπορεί να καταλήξει να παρέχει ζωτικής σημασίας προσωπικές πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν για phishing ή κλοπή ταυτότητας από μη αξιόπιστους ιστότοπους.

Επιπλέον, η αυξανόμενη χρήση του διαδικτύου συμβάλλει σε δυσμενείς επιπτώσεις, συμπεριλαμβανομένης της ανάπτυξης εθισμών, όπως είναι για παράδειγμα τα τυχερά παιχνίδια και ο τζόγος, και του διαδικτυακού εκφοβισμού. Τέτοια ζητήματα θα πρέπει να περιοριστούν σε πρώιμο στάδιο για να διασφαλιστεί ότι έχουν περιορισμένες επιπτώσεις στους χρήστες του Διαδικτύου. Ο καλύτερος τρόπος διαχείρισης αυτών των διαδικτυακών απειλών είναι η ενσωμάτωση της εκπαίδευσης στον κυβερνοχώρο σε εκπαιδευτικά ιδρύματα, όπου οι μαθητές μαθαίνουν αρκετά νωρίς πώς να εντοπίζουν πιθανές απάτες ή

απειλές καθώς επίσης και την ηθική της αλληλεπίδρασης με άλλα άτομα στο διαδίκτυο. Σε αυτόν τον βαθμό, η γνώση της κυβερνοασφάλειας είναι ζωτικής σημασίας για τους χρήστες του Διαδικτύου. Μέσα από τη γνώση αυτή είναι δυνατό να μαθαίνονται τρόποι αντίδρασης σε απειλές στον κυβερνοχώρο. Με τον τρόπο αυτό οι άνθρωποι έχουν μειωμένες πιθανότητες για επιπτώσεις μέσα από τις απειλές στον κυβερνοχώρο [13]. Η έρευνα δείχνει επίσης ότι τα εγκλήματα στον κυβερνοχώρο μπορούν να συμβούν ανά πάσα στιγμή, ανεξάρτητα από οργανισμούς, μέρη και άτομα. Ως εκ τούτου, αυτό απαιτεί την εφαρμογή της γνώσης για την ασφάλεια στον κυβερνοχώρο σε όλα τα επίπεδα των εκπαιδευτικών ιδρυμάτων [14].

Είναι σημαντικό να υπάρχει προστασία από τη μη εξουσιοδοτημένη χρήση ηλεκτρονικών δεδομένων και πρόσβαση εγκληματιών στον κυβερνοχώρο. Αυτό, ονομάζεται κυβερνοασφάλεια [14]. Η κυβερνοασφάλεια, λοιπόν, καλύπτει τα μέτρα που λαμβάνονται για τη διασφάλιση της ασφάλειας από τα εγκλήματα στον κυβερνοχώρο. Η ενσωμάτωση της γνώσης της κυβερνοασφάλειας μέσα στα σχολεία μπορεί να καλλιεργήσει μια κουλτούρα που αγκαλιάζει την ηθική χρήση του Διαδικτύου από νεαρή ηλικία. Μέσα από τον τρόπο αυτό, όλες εκείνες οι αρνητικές επιπτώσεις που απορρέουν από τα εγκλήματα του κυβερνοχώρου είναι δυνατό να μετριάσουν [15].

Η ραγδαία ανάπτυξη της Τεχνολογίας Πληροφορίας και Επικοινωνιών, έχει οδηγήσει σε δραστικές αλλαγές στη ζωή των ανθρώπων. Η επικοινωνία είναι πολύ πιο αποτελεσματική ανεξάρτητα από γεωγραφικά όρια και οι πληροφορίες είναι άμεσα διαθέσιμες σε όλους από κάθε σημείο του πλανήτη. Ακόμα σημαντικό, είναι η πρόοδος της τεχνολογίας η οποία έχει βοηθήσει στην ανάπτυξη μιας κοινωνίας που αγκαλιάζει την καινοτομία και τις εφευρέσεις. Μέσω της ανταλλαγής ιδεών, οι χρήστες του Διαδικτύου μπορούν εύκολα να αναπτύξουν λύσεις σε κρίσιμα προβλήματα. Από την άλλη, βέβαια, οι εγκληματίες μπορούν να εκμεταλλευτούν αυτές τις εξελίξεις για να επινοήσουν νέους τρόπους εκτέλεσης των εγκλημάτων στον κυβερνοχώρο, διασφαλίζοντας παράλληλα την ανωνυμία καθώς επίσης και τη δυνατότητα μη εντοπισμού τους από τις αρχές [16]. Για τους χρήστες του Microsoft Word ή κάποιου συμβατού προγράμματος, συστήνεται η χρήση του παρόντος δείγματος ως βάση. Με την επιλογή της χρήσης των «styles» του Microsoft Word, μπορεί να επιτευχθεί γρήγορη μορφοποίηση του κειμένου.

Η κυβερνοασφάλεια, ακόμα, αποτελεί τη διαδικασία, την κατάσταση ή τη δραστηριότητα κατά την οποία τα συστήματα επικοινωνίας και οι πληροφορίες προστατεύονται από τροποποίηση, μη εξουσιοδοτημένη πρόσβαση ή εκμετάλλευση. Ως εκ τούτου, η γνώση της κυβερνοασφάλειας μπορεί να βοηθήσει στην αποτροπή των ανθρώπων από απειλές στον κυβερνοχώρο, όπως είναι για παράδειγμα τα ransomware [14]. Τα παιδιά, πολλές φορές, έρχονται αντιμέτωπα με πολυάριθμες απειλές, όπως περιεχόμενο για ενηλίκους που μπορεί να συναντήσουν σε παιχνίδια και βίντεο. Γενικότερα, μέσα από τις απειλές αυτές, είναι

δυνατό να επηρεαστεί σε αρνητικό βαθμό η ψυχική τους υγεία. Σε αυτόν τον βαθμό, οι γονείς μέσα από τη γνώση της κυβερνοασφάλειας, είναι δυνατό να συμβάλουν στην προστασία των παιδιών τους από επιβλαβές διαδικτυακό περιεχόμενο [17]. Ένας τρόπος για να εφαρμοστεί η προστασία αυτή είναι να γίνει εγκατάσταση γονικών ελέγχων σε συσκευές όπως π.χ. τηλεοράσεις και τηλέφωνα. Με αυτό τον τρόπο μπορεί να γίνει περιορισμός των παιδιών από επιβλαβές περιεχόμενο.

Μιλώντας, πάλι, από τη θετική του μεριά, τα παιδιά μπορούν να χρησιμοποιήσουν το Διαδίκτυο για να αποκτήσουν πρόσβαση σε πολλά βιβλία και περιοδικά ζωτικής σημασίας για την εκπαίδευσή τους και τελικά να διευρύνουν τις γνώσεις και την εξειδίκευσή τους. Για παράδειγμα, το YouTube είναι γεμάτο από εκπαιδευτικά βίντεο που μπορούν να βοηθήσουν τους ανθρώπους να αντιμετωπίσουν κοινά προβλήματα στην καθημερινή τους ζωή. Το πιο σημαντικό, οι άνθρωποι χρειάζονται δεξιότητες και γνώσεις στα Αγγλικά για να παίξουν παιχνίδια για να κατανοήσουν τις διαδικασίες και τις ρυθμίσεις των παιχνιδιών [18]. Επομένως, τα παιχνίδια συχνά ενθαρρύνουν την πρόοδο και την ανάπτυξη της ομιλίας, της γραφής και της ανάγνωσης στα αγγλικά. Ωστόσο, τέτοια παιχνίδια συχνά ενθαρρύνουν την τεμπελιά μεταξύ των παιδιών καθώς περνούν πολλές ώρες προσπαθώντας να ολοκληρώσουν τα διάφορα επίπεδα.

2.2 Εννοιολογικοί Ορισμοί

2.2.1 Ορισμός Κυβερνοασφάλειας

Υπάρχουν διάφοροι ορισμοί σχετικά με την κυβερνοασφάλεια. Κάποιοι από αυτούς περιγράφονται σε αυτό το εδάφιο.

Σύμφωνα με τους Seema et al., η κυβερνοασφάλεια αποτελεί την προστασία των συστημάτων που είναι συνδεδεμένα στο Διαδίκτυο, συμπεριλαμβανομένου υλικού, λογισμικού και δεδομένων, από επιθέσεις στον κυβερνοχώρο. Σε ένα υπολογιστικό πλαίσιο, η ασφάλεια περιλαμβάνει την ασφάλεια στον κυβερνοχώρο και τη φυσική ασφάλεια και οι δύο χρησιμοποιούνται από τις επιχειρήσεις για την προστασία από μη εξουσιοδοτημένη πρόσβαση σε κέντρα δεδομένων και άλλα ηλεκτρονικά συστήματα. Η ασφάλεια, η οποία έχει σχεδιαστεί για να διατηρεί την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, αποτελεί υποσύνολο της ασφάλειας στον κυβερνοχώρο [19].

Ένας άλλος ορισμός της κυβερνοασφάλειας, ορίζει την κυβερνοασφάλεια ως την οργάνωση και συλλογή πόρων, διαδικασιών και δομών που χρησιμοποιούνται για την προστασία του κυβερνοχώρου και των συστημάτων που υποστηρίζουν τον κυβερνοχώρο από περιστατικά που δεν ευθυγραμμίζονται de jure με τα de facto δικαιώματα ιδιοκτησίας [20].

2.3 Ασφάλεια Στο Διαδίκτυο

Η πρόσβαση στο Διαδίκτυο είναι πανταχού παρούσα στις μέρες μας. Αυτή η πρόσβαση είναι διαθέσιμη όχι μόνο σε ενήλικες, αλλά και δυστυχώς ή ευτυχώς σε παιδιά. Από μικρή ηλικία, τα παιδιά έχουν συνηθίσει σε «λαμπερές οθόνες» και όλο και μικρότερα παιδιά μαθαίνουν πώς να χρησιμοποιούν αυτά τα σύγχρονα οφέλη του 21ου αιώνα. Στο παρελθόν, δεν υπήρχαν τόσα πολλά προβλήματα σχετικά με το Διαδίκτυο και τη δραστηριότητα των παιδιών σε αυτό, επειδή το ίδιο το Διαδίκτυο δεν ήταν διαθέσιμο σε όλους. Λόγω της ταχείας δυναμικής της τεχνολογικής αλλαγής, τα παιδιά άρχισαν να τη χρησιμοποιούν πιο ελεύθερα και πιο συχνά. Παράλληλα με την ευρύτερη πρόσβαση στο Διαδίκτυο, έχει αρχίσει να εμφανίζεται εκεί περιεχόμενο και διάφορα είδη απειλών, από τα οποία θα πρέπει να προστατεύονται τα παιδιά. Ως εκ τούτου, είναι πολύ σημαντικό να εκπαιδεύονται σε αυτό το θέμα από μικρή ηλικία [21].

Ο όρος «ασφάλεια στο Διαδίκτυο» περιλαμβάνει ένα σύνολο θεμάτων που σχετίζονται, άμεσα ή έμμεσα, με τη σωματική καθώς επίσης και με τη ψυχολογική ευημερία των χρηστών του Διαδικτύου. Αναφέρεται επίσης ως "ασφάλεια στο διαδίκτυο", "ψηφιακή ασφάλεια" ή "ηλεκτρονική ασφάλεια". Αυτή η έννοια σχετίζεται τόσο με τους κινδύνους που αντιμετωπίζουν τα άτομα στο διαδίκτυο όσο και με τους τρόπους με τους οποίους μπορούν να προστατευτούν. Είναι αξιοσημείωτο το γεγονός ότι έχει γίνει αρκετή έρευνα αφιερωμένη στην ασφάλεια των παιδιών και των εφήβων. Ένας λόγος για τη συγκεκριμένη εστίαση είναι το γεγονός ότι οι νέοι είναι οι πιο ενεργοί χρήστες του Διαδικτύου. Το να είναι online τους προσφέρει μια σειρά από ευκαιρίες, αλλά ταυτόχρονα, αυτό, μπορεί να τους αντιμετωπίσει πολλούς κινδύνους. Οι έφηβοι μπορεί να είναι ιδιαίτερα ευάλωτοι όταν αντιμετωπίζουν αυτούς τους διαδικτυακούς κινδύνους σε σύγκριση με τους ενήλικες. Μια επιπλέον ανησυχία που σχετίζεται με αυτήν την ηλικιακή ομάδα είναι ότι ο τρόπος με τον οποίο έχουν πρόσβαση στο Διαδίκτυο διαφέρει από τις προηγούμενες γενιές. Οι περισσότερες συσκευές που χρησιμοποιούνται για σύνδεση στο διαδίκτυο έχουν γίνει φορητές και, ως εκ τούτου, οι νέοι περνούν όλο και περισσότερο χρόνο μόνοι τους με τους φορητούς υπολογιστές, τα smartphone και τα tablet τους, για παράδειγμα στα υπνοδωμάτιά τους. Κατά συνέπεια, η χρήση του Διαδικτύου από τα παιδιά γίνεται τις περισσότερες φορές χωρίς γονική επίβλεψη [21].

Αν και οι περισσότερες μελέτες επικεντρώνονται στη διαδικτυακή συμπεριφορά των νέων, παρόλα αυτά, δεν σημαίνει ότι οι ενήλικες δεν είναι επιρρεπείς στον διαδικτυακό κίνδυνο. Μπορεί να είναι λιγότερο ευάλωτοι σε ορισμένους κινδύνους και λιγότερο επιρρεπείς στο να αναλάβουν κινδύνους γενικά, αλλά δεν είναι απρόσβλητοι από τις

δυνητικά αρνητικές συνέπειες που σχετίζονται με την επικίνδυνη χρήση του Διαδικτύου, όπως ζημιά στη φήμη ή απώλεια χρημάτων μέσω διαδικτυακών απατών. Επιπλέον, έχει φανεί μέσα από έρευνα ότι οι μεγαλύτεροι σε ηλικία χρήστες του Διαδικτύου τείνουν να έχουν λιγότερη εμπειρία με διάφορους τύπους και λειτουργίες τεχνολογίας, υπονοώντας ότι οι μεγαλύτεροι Οι χρήστες μπορεί να είναι εξίσου ευάλωτοι στο διαδίκτυο με τους νεότερους ομολόγους τους σε ορισμένες περιπτώσεις [22].

Ένας αριθμός διαφορετικών κατηγοριοποιήσεων χρησιμοποιούνται για την ταξινόμηση των διαδικτυακών κινδύνων. Μια συχνά εφαρμοζόμενη κατηγοριοποίηση δημιουργήθηκε στο πλαίσιο του έργου EU Kids Online η οποία έχει κάνει διάκριση των κινδύνων σε επιθετικούς, σεξουαλικούς, εμπορικούς και αξιακούς κινδύνους [23]. Σε μια δεύτερη κατηγοριοποίηση, μπορεί να γίνει διάκριση μεταξύ των κινδύνων που σχετίζονται με το διαδικτυακό περιεχόμενο και εκείνων που σχετίζονται με την διαδικτυακή επαφή [24]. Οι κίνδυνοι επαφής προϋποθέτουν μια άμεση σύνδεση ή αλληλεπίδραση μεταξύ δράστη και θύματος, ενώ αυτού του είδους η σύνδεση απουσιάζει ή είναι λιγότερο ορατή όταν αντιμετωπίζουμε κινδύνους περιεχομένου. Είναι σημαντικό να σημειωθεί ότι μπορεί να υπάρχει επικάλυψη μεταξύ ορισμένων κατηγοριών, π.χ. μεταξύ επιθετικού περιεχομένου και ορισμένων κινδύνων που σχετίζονται με την αξία. Επιπλέον, ορισμένοι κίνδυνοι μπορεί να συνυπάρχουν σε συγκεκριμένα διαδικτυακά πλαίσια όπως είναι για παράδειγμα η ρητορική μίσους που θα μπορούσε να οδηγήσει σε διαδικτυακό εκφοβισμό.

Για τα παιδιά, το Διαδίκτυο είναι μια σημαντική πηγή μάθησης, προσωπικής ανάπτυξης ή κοινωνικοποίησης και ψυχαγωγίας. Την ίδια στιγμή, το Διαδίκτυο, είναι επίσης ένα περιβάλλον όπου υπάρχουν κίνδυνοι στον ίδιο βαθμό, αν όχι σε μεγαλύτερο βαθμό, από ό,τι στην πραγματική ζωή. Όπως έχουν δείξει προηγούμενες μελέτες, «οι διαδικτυακές δραστηριότητες δεν είναι από μόνες τους ωφέλιμες ή επιβλαβείς για τα παιδιά» και «οι ευκαιρίες και οι κίνδυνοι πάνε χέρι-χέρι» [26].

Τόσο η ταχεία ανάπτυξη συσκευών συνδεδεμένων στο Διαδίκτυο και η εύκολη και γρήγορη πρόσβαση στο Διαδίκτυο, όσο και το αυξανόμενο ενδιαφέρον των παιδιών για τη χρήση τους, που θέλουν να καρπωθούν όλα τα οφέλη μιας «συνδεδεμένης» ζωής [27], συμβάλλουν στην παρουσία ο αυξανόμενου αριθμού ανηλίκων στο Διαδίκτυο, ενώ τους εκθέτει και στους κινδύνους που ενέχει το διαδικτυακό περιβάλλον, από τη μόλυνση των συσκευών τους με κακόβουλο λογισμικό και την κλοπή πληροφοριών από αυτούς, μέχρι πιο σοβαρές πράξεις όπως ο εκβιασμός και η διαδικτυακή παιδική πορνογραφία [28].

2.4 Ανασκόπηση Ερευνητικής Βιβλιογραφίας

2.2.1 Η διδασκαλία της Κυβερνοασφάλειας

Για τους σκοπούς της παρούσας μελέτης, έχουν αναλυθεί συνολικά 14 ερευνητικά άρθρα σχετικά με τη διδασκαλία της κυβερνοασφάλειας στα σχολεία.

Η κυβερνοασφάλεια είναι ζωτικής σημασίας για την εθνική υποδομή, την ομοσπονδιακή και τοπική κυβέρνηση, τον στρατό, τη βιομηχανία και το προσωπικό απόρρητο. Για την υπεράσπιση των ΗΠΑ έναντι των απειλών στον κυβερνοχώρο, προβλέπεται σημαντική ζήτηση για εξειδικευμένο εργατικό δυναμικό στον τομέα της κυβερνοασφάλειας σε κυβερνητικούς και βιομηχανικούς τομείς.

Αρχικά, στην έρευνα των Jin et al., ο σκοπός ήταν να δημιουργηθεί το πρόγραμμα GenCyber για την τόνωση του ενδιαφέροντος των μαθητών K-12 στον τομέα της κυβερνοασφάλειας και να αυξηθεί η ευαισθητοποίηση του για την ασφάλεια στον κυβερνοχώρο καθώς επίσης και στην ασφαλή διαδικτυακή συμπεριφορά. Για το σκοπό της έρευνας αυτής, το Πανεπιστήμιο Purdue Northwest ξεκίνησε με επιτυχία τέσσερις θερινές κατασκηνώσεις GenCyber το 2016 και το 2017 σε 181 μαθητές γυμνασίου. Στους συμμετέχοντες δόθηκαν δραστηριότητες καλοκαιρινής κατασκήνωσης GenCyber με τη μορφή μάθησης βασισμένης σε παιχνίδια και πρακτικών εργαστηρίων. Η χρήση της μάθησης με βάση το παιχνίδι στην κατασκήνωση ήταν μια πλατφόρμα για τη διδασκαλία των αρχών της ασφάλειας στον κυβερνοχώρο. Για παράδειγμα, στο Cyber Defense Tower Game, οι μαθητές έπρεπε να προστατεύουν τους διακομιστές τους από τους διαφορετικούς τύπους κυβερνοεπιθέσεων, επιλέγοντας το σωστό τύπο άμυνας. Καθώς οι μαθητές προχωρούσαν στο παιχνίδι, οι συνδυασμοί των διαφορετικών επιθέσεων θα ερχόντουσαν πιο γρήγορα, καθιστώντας πιο δύσκολο για τους μαθητές να υπερασπιστούν τους διακομιστές τους. Αυτό το παιχνίδι έτυχε καλής υποδοχής από τους μαθητές, το προσωπικό υποστήριξης και τους εκπαιδευτές. Συνεπώς, μέσα από τα αποτελέσματα της έρευνας αυτής έχει φανεί ότι η μάθηση μέσω αυτών των δραστηριοτήτων παρείχε στους μαθητές γυμνασίου μια καθηλωτική, μαθητοκεντρική εμπειρία, η οποία έχει αποδειχθεί πολύ αποτελεσματική στην εκπαίδευση ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο και στην απόκτηση πρακτικών δεξιοτήτων για μαθητές από διαφορετικά υπόβαθρα [21].

Σε μια άλλη όμοια έρευνα, αυτή των Olano et al., ο σκοπός ήταν να δημιουργηθεί ένα παιχνίδι το οποίο ευαισθητοποιεί τους μαθητές σχετικά με τις πρακτικές ασφάλειας στον κυβερνοχώρο. Το SecurityEmpire ήταν ένα νέο παιχνίδι υπολογιστή για πολλούς παίκτες το οποίο δίδασκε έννοιες κυβερνοασφάλειας σε μαθητές γυμνασίου. Το SecurityEmpire

προκαλεί κάθε χρήστη να δημιουργήσει μια εταιρεία πράσινης ενέργειας, ενώ παράλληλα συμμετέχει σε ορθές πρακτικές διασφάλισης πληροφοριών και αποφεύγοντας λάθη ασφαλείας. Οι πρακτικές διασφάλισης υγιών πληροφοριών περιλαμβάνουν: μη κλικ σε μη ασφαλείς συνδέσμους, κρυπτογράφηση προσφορών δημοπρασίας, έλεγχο ταυτότητας λήψεων λογισμικού, εκτέλεση ελέγχων ακεραιότητας λογισμικού συστήματος, ενημερωμένη προστασία προστασίας από ιούς και επιλογή ισχυρών κωδικών πρόσβασης. Σε αντίθεση με τις παραδοσιακές μεθόδους διδασκαλίας, τα εκπαιδευτικά παιχνίδια υπόσχονται μεγαλύτερη συμμετοχή και μάθηση των μαθητών. Στην έρευνα αυτή δοκιμάστηκε πιλοτικά μια αρχική έκδοση του παιχνιδιού σε μαθήματα πληροφορικής σε συνεργαζόμενα λύκεια και σε προπτυχιακό μάθημα gaming σε πανεπιστήμιο. Μέσα από τα αποτελέσματα της έρευνας αυτής έχει φανεί ότι το παιχνίδι είναι ελκυστικό και αυξάνει την ευαισθητοποίηση σχετικά με τις πρακτικές ασφάλειας στον κυβερνοχώρο [22].

Όμοια, στην έρευνα των Lendezci et al., ο σκοπός ήταν να αναπτυχθεί ένα ρομπότ το οποίο κάνει τις βασικές ιδέες στην επιστήμη των υπολογιστών προσιτές σε ομάδες μαθητών K-12 να ευαισθητοποιούνται στην ασφάλεια στον κυβερνοχώρο. Το RoboScape παρέχει μια ανατροπή στην τελευταία λέξη της τεχνολογίας των πλατφορμών εκμάθησης ρομποτικής. Πρώτον, το πρόγραμμα ενός χρήστη που ελέγχει το ρομπότ εκτελείται στο πρόγραμμα περιήγησης και όχι στο ρομπότ. Δεύτερον, η ασύρματη επικοινωνία μεταξύ του προγράμματος ενός μαθητή και του ρομπότ μπορεί να ακουστεί από τα προγράμματα των άλλων μαθητών. Αυτό καθιστά την ασφάλεια στον κυβερνοχώρο μια άμεση ανάγκη που οι μαθητές αντιλαμβάνονται και μπορούν να εργαστούν για να αντιμετωπίσουν. Το πρόγραμμα σχεδιάστηκε και παραδόθηκε σε μια καλοκαιρινή κατασκήνωση κυβερνοασφάλειας σε 24 μαθητές K-12 [23].

Σε μια άλλη έρευνα, αυτήν των Jones et al., ο σκοπός ήταν να προσδιοριστούν οι γνώσεις οι δεξιότητες και οι ικανότητες που πρέπει να συμπεριλαμβάνονται στην εκπαίδευση και κατάρτιση στον κυβερνοχώρο. Το δείγμα της έρευνας αυτής αποτελείτο από 44 επαγγελματίες ασφάλειας που συμμετείχαν σε κορυφαία συνέδρια hacking Black Hat και DEF CON. Το μέσο συλλογής δεδομένων που χρησιμοποιήθηκε στην έρευνα αυτή ήταν η συνέντευξη στην οποία περιλαμβάνονταν 32 σημεία γνώσεων, δεξιοτήτων και ικανοτήτων σχετικά με την κυβερνοασφάλεια. Τα αποτελέσματα της έρευνας αυτής έχουν δείξει ότι 15 από τα σημεία αυτά έχουν αξιολογηθεί ως μεγαλύτερης σημασίας και αφορούσαν δίκτυα, π.χ. γνώση πρωτοκόλλων δικτύου καθώς επίσης και απειλές, π.χ. γνώση των τύπων απειλών και τρωτών σημείων ασφαλείας. Επίσης, έχει φανεί ότι 31

από τα 32 σημεία, ήταν γνώρισμα για τους συμμετέχοντες. Συνεπώς, μέσα από τα αποτελέσματα της έρευνας αυτής έχει φανεί ότι πρέπει να δίνεται έμφαση στην απόκτηση γνώσεων, δεξιοτήτων και ικανοτήτων που αφορούν τα δίκτυα κατά την εκπαίδευση στα σχολεία. Επίσης είναι σημαντικό να δίνεται προτεραιότητα στην απόκτηση γνώσεων, δεξιοτήτων και ικανοτήτων για απειλές και ευπάθειες [22].

Είναι αξιοσημείωτο, επίσης, το γεγονός ότι η υπόθεση Megan Meier του 2006, όπου μια έφηβη που δεχόταν εκφοβισμό στο Διαδίκτυο μέσω e-mail και Myspace, η οποία λέγεται ότι τελικά οδήγησε στην αυτοκτονία της, έριξε φως στο ζήτημα του διαδικτυακού εκφοβισμού στα σχολεία. Η έρευνα των Chen et al., είχε σκοπό να περιγράψει πώς πολλά σχολικά ιδρύματα αντιμετώπιζαν την απώλεια εμπιστευτικών πληροφοριών και προστατεύοντας τους μαθητές στο WWW, το καθένα μέσα από ένα μοναδικό σύνολο περιστάσεων. Η έρευνα αυτή αποτελεί μια προσέγγιση μελέτης περίπτωσης. Μέσα από την έρευνα αυτή αποκαλύπτονται αντιδράσεις των θεσμών και τρόποι αντιμετώπισης των απειλών στον κυβερνοχώρο. Με τις εμπειρίες, οι σχολικές περιφέρειες είναι σημαντικό λαμβάνουν μέτρα για να προσφέρουν εκπαίδευση αξίας βελτιώνοντας τις γνώσεις και την επίγνωση των μαθητών σχετικά με τις έννοιες της Κυβερνοηθικής, της Κυβερνοασφάλειας και της Κυβερνοασφάλειας για να τους παρέχουν τα μέσα για να προστατευθούν και να ενισχύσουν την ασφάλεια και την ασφάλεια των εθνικών υποδομών [23].

Τις τελευταίες δεκαετίες, η κυβερνοηθική, η κυβερνοασφάλεια και η ασφάλεια στον κυβερνοχώρο αποτελούν το επίκεντρο του ενδιαφέροντος στα σχολεία.

Στην έρευνα των Chen et al., ο σκοπός ήταν να περιγραφεί το ζήτημα της κυβερνοηθικής, της κυβερνοασφάλειας και της ασφάλειας στον κυβερνοχώρο (3Cs), καθώς και πώς τα προβλήματα αυτών των τριών αναμειγνύονται για να γίνουν γενικά ζητήματα κυβερνοηθικής για την κοινωνία. Η έρευνα αυτή αποτελεί μελέτη περίπτωσης. Μέσα από την έρευνα αυτή προωθούνται οι καλοί κυβερνοπολίτες στα σχολεία επειδή είναι πολύ σημαντικό για τις σχολικές περιφέρειες να λάβουν ορισμένα μέτρα για τη βελτίωση της γνώσης και της ευαισθητοποίησης των μαθητών σχετικά με την κυβερνοηθική, την ασφάλεια στον κυβερνοχώρο και την ασφάλεια στον κυβερνοχώρο, για την ενίσχυση της ασφάλειας και της ασφάλειας της σχολικής υποδομής, για την αποφυγή του διαδικτυακού εκφοβισμού , για να διασφαλιστεί ότι οι μαθητές είναι καλοί πολίτες στον κυβερνοχώρο και να βοηθήσουν στην εκπαίδευση των δασκάλων να είναι επαγγελματίες του κυβερνοχώρου [24].

Όπως έχει αναφερθεί και προηγουμένως, υπάρχει μια αυξανόμενη τάση που παροτρύνει τους ανθρώπους να χρησιμοποιούν δεδομένα. Ωστόσο, η πιθανότητα κακόβουλης χρήσης δεδομένων που αποκαλύπτονται στο διαδίκτυο απαιτεί προσοχή. Η επικίνδυνη συμπεριφορά ασφάλειας πληροφοριών συχνά οδηγεί σε ζημιά. Για τους μαθητές πρωτοβάθμιας και δευτεροβάθμια ηλικίας, οι δάσκαλοί τους μπορούν να λειτουργήσουν ως πρότυπα. Μέσω της κατανόησης των συμπεριφορικών προθέσεων των εκπαιδευτικών για την ασφάλεια των πληροφοριών και των σχετικών κινήτρων προστασίας, μπορούν να σχεδιαστούν προγράμματα κατάρτισης για εκπαιδευτικούς και, ως εκ τούτου, να αυξηθεί η κανονιστική κρίση των δασκάλων καθώς και των μαθητών σχετικά με τη συμπεριφορά ασφάλειας πληροφοριών.

Στην έρευνα των Chou et al., ο σκοπός ήταν να διερευνηθούν οι παράγοντες που σχετίζονται με τη συμπεριφορά των εκπαιδευτικών στην ασφάλεια των πληροφοριών, όπως βασίζεται στη Θεωρία Κίνητρων Προστασίας. Στην έρευνα αυτή έλαβαν μέρος 505 συμμετέχοντες. Μέσα από τα αποτελέσματα της έρευνας αυτής έχει φανεί ότι όσοι αντιλήφθηκαν τα περιστατικά ασφάλειας στο Διαδίκτυο ως σοβαρά εμπλέκονταν σε λιγότερο προβληματική συμπεριφορά InfoSec σε σύγκριση με εκείνους που θεωρούσαν ότι τα περιστατικά δεν ήταν τίποτα σοβαρά. Στην παρούσα έρευνα, αναπτύχθηκε μια κλίμακα για τη μέτρηση των αντιλήψεων των εκπαιδευτικών για τα κίνητρα προστασίας και την προβληματική συμπεριφορά InfoSec με βάση προηγούμενες σχετικές έρευνες. Εξήχθησαν πέντε παράγοντες: η αντιληπτή σοβαρότητα, η αντιληπτή ευαλωτότητα, η αποτελεσματικότητα απόκρισης, το κόστος απόκρισης και η αυτοαποτελεσματικότητα [25].

Επιπρόσθετα, η έρευνα των Javidi et al., αφορά μια νέα προσέγγιση στην εκπαίδευση για την ασφάλεια στον κυβερνοχώρο. Η συναίνεση στην κοινότητα STEM είναι ότι το πρόβλημα ξεκινά στα σχολεία k-12 με πολύ λίγους μαθητές που ενδιαφέρονται για τα θέματα STEM. Σκοπός της έρευνας αυτής ήταν να γίνει προώθηση ερευνητικών ατζεντών σχετικά με την κυβερνοασφάλεια και να εκπαιδευτεί η μελλοντική γενιά σε θέματα δεξιοτήτων στην κυβερνοασφάλεια. Οι δεξιότητες ηγεσίας και επιχειρηματικότητας προστίθενται επίσης στο μείγμα για να προετοιμαστούν οι μαθητές για προβλήματα του πραγματικού κόσμου. Η εκπαίδευση στην κυβερνοασφάλεια αποτελεί ένα νέο μοντέλο εκπαίδευσης [26].

Ακόμα, η έρευνα του Haseski είχε στόχο να προσδιορίσει την επίδραση των ατομικών δεξιοτήτων ασφάλειας στον κυβερνοχώρο των εκπαιδευτικών και τη στάση τους απέναντι στην εκπαίδευση με τη βοήθεια υπολογιστή. Η παρούσα έρευνα αποτελεί

μελέτη συσχέτισης στην οποία έλαβαν μέρος 241 καθηγητές σε διαφορετικά τμήματα στο Πανεπιστήμιο Manisa Celal Bayar, κατά το ακαδημαϊκό έτος 2019-2020 το χειμερινό εξάμηνο. Τα δεδομένα συλλέχθηκαν με την "Προσωπική Κλίμακα Παροχής Ασφάλειας στον Κυβερνοχώρο" και "Η Κλίμακα Στάσης προς την Εκπαίδευση Υποβοηθούμενη από Υπολογιστή". Με βάση τα ευρήματα της μελέτης, οι εκπαιδευτικοί θα πρέπει να βελτιώσουν τις ικανότητές τους στην ασφάλεια στον κυβερνοχώρο. Επιπλέον, οι εκπαιδευτικοί που είχαν προσωπικό υπολογιστή είχαν υψηλότερες βαθμολογίες στη διατήρηση της προσωπικής ασφάλειας στον κυβερνοχώρο και είχαν καλύτερη στάση απέναντι στην εκπαίδευση με τη βοήθεια υπολογιστή. Επιπλέον, παρατηρήθηκε ότι υπήρχαν διαφορές μεταξύ των προσωπικών βαθμολογιών ασφάλειας στον κυβερνοχώρο των εκπαιδευτικών προϋπηρεσίας και της στάσης τους απέναντι στην εκπαίδευση με τη βοήθεια υπολογιστή βάσει των τμημάτων τους. Επιπλέον, εντοπίστηκε ότι η βαθμολογία επιτευγμάτων προσωπικής ασφάλειας στον κυβερνοχώρο ήταν ένας σημαντικός παράγοντας πρόβλεψης της στάσης απέναντι στην εκπαίδευση με τη βοήθεια υπολογιστή [27].

Αυτή η δραστηριότητα αντιπροσωπεύει επομένως ένα θεμελιώδες βήμα για την εκπαίδευση στον κυβερνοχώρο.

Ακόμα, στην έρευνα των Corrandini et al., (2020) ο σκοπός ήταν η διερεύνηση των αντιλήψεων των εκπαιδευτικών σε σχολεία της Ιταλίας για την ψηφιακή επίγνωση των μαθητών τους και την αξιολόγησή τους για τις ενέργειες που απαιτούνται για την ανάπτυξή της. Στην έρευνα αυτή έλαβαν μέρος 2.229 εκπαιδευτικοί από όλη τη χώρα που ανήκουν σε σχολεία πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, συμμετέχοντας σε ένα εθνικό πρόγραμμα που στόχο έχει τη διάδοση της επιστήμης των υπολογιστών και την ευαισθητοποίηση των μαθητών στη σωστή χρήση των ψηφιακών τεχνολογιών. Τα αποτελέσματα της έρευνας αυτής επιβεβαιώνουν την υψηλή ευαισθησία των εκπαιδευτικών σε θέματα ψηφιακής ευαισθητοποίησης. Επιπλέον, οι εκπαιδευτικοί δηλώνουν την ανάγκη να λάβουν οι ίδιοι ειδική εκπαίδευση για την ψηφιακή ευαισθητοποίηση και να υποστηριχθούν στις δραστηριότητές τους [28].

Επιπρόσθετα, η έρευνα του Caparino, είχε σκοπό τη διερεύνηση των αντιλήψεων για την ασφάλεια στον κυβερνοχώρο μεταξύ των εκπαιδευτικών. Στην έρευνα αυτή έλαβαν μέρος 84 εκπαιδευτικοί οι οποίοι κλήθηκαν να συμπληρώσουν ένα ερωτηματολόγιο. Τα αποτελέσματα αυτής της μελέτης θα βοηθούσαν τις αρμόδιες αρχές να μην περιορίζονται στους διαχειριστές ιδρυμάτων μέσης και τριτοβάθμιας εκπαίδευσης στην ανάπτυξη προγραμμάτων για την ασφάλεια στον κυβερνοχώρο μεταξύ των εκπαιδευτικών [29].

Η ευαισθητοποίηση σχετικά με την ασφάλεια των πληροφοριών μπορεί να διαδραματίσει σημαντικό ρόλο στην αντιμετώπιση επιθέσεων στον κυβερνοχώρο από εισβολείς. Στην έρευνα των Al-Janabi et al., ο σκοπός ήταν να αναλύσει την ευαισθητοποίηση για την ασφάλεια των πληροφοριών μεταξύ του ακαδημαϊκού προσωπικού, ερευνητών, προπτυχιακών φοιτητών και εργαζομένων σε εκπαιδευτικά περιβάλλοντα στη Μέση Ανατολή σε μια προσπάθεια κατανόησης του επιπέδου συνειδητοποίησης της ασφάλειας των πληροφοριών, των σχετικών κινδύνων και του συνολικού αντίκτυπου στην τους θεσμούς. Τα αποτελέσματα της έρευνας αυτής έχουν δείξει ότι οι συμμετέχοντες δεν είχαν την απαιτούμενη γνώση και κατανόηση της σημασίας των αρχών ασφάλειας πληροφοριών και της πρακτικής εφαρμογής τους στην καθημερινή τους εργασία. Αυτή η κατάσταση μπορεί ωστόσο να διορθωθεί μέσω ολοκληρωμένων προγραμμάτων ευαισθητοποίησης και κατάρτισης καθώς και με την υιοθέτηση όλων των απαραίτητων μέτρων ασφαλείας σε όλα τα επίπεδα του ιδρύματος για να διασφαλιστεί ότι οι φοιτητές, το ακαδημαϊκό προσωπικό και οι εργαζόμενοι είναι αξιόπιστοι, γνωρίζουν την τεχνολογία και διατηρούν τα δεδομένα τους ασφαλή. Χωρίς τέτοια προγράμματα εκπαίδευσης και ευαισθητοποίησης, θα υπάρξουν αρνητικές συνέπειες στα συστήματα πληροφορικής και στη χρήση των εφαρμογών τους, καθώς και στην προσωπική ασφάλεια των χρηστών τώρα και στο μέλλον [30].

Η ασφάλεια στον κυβερνοχώρο θεωρείται αναγκαιότητα για οποιονδήποτε στο σύγχρονο σύγχρονο κόσμο. Η επίγνωση των προτύπων και των βέλτιστων πρακτικών ασφάλειας στον κυβερνοχώρο έχει γίνει υποχρεωτική για την προστασία των παιδιών σε αυτήν την εποχή. Σήμερα, οι μαθητές γυμνασίου δεν κατανοούν τις απειλές για την ασφάλεια στον κυβερνοχώρο λόγω της έλλειψης συμμετοχής των γονέων ή της εκπαίδευσης στο γυμνάσιο.

Στην έρευνα των Al-Tajer et al., ο σκοπός ήταν να αναπτυχθεί ένα πλαίσιο που αντιμετωπίζει την έλλειψη ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο για τους μαθητές γυμνασίου. Το προτεινόμενο πλαίσιο παρείχε μια ροή βημάτων για την παροχή αποτελεσματικών προσεγγίσεων ευαισθητοποίησης για το k12. Αυτό επιτεύχθηκε χρησιμοποιώντας μια προσέγγιση δημιουργίας ενός λειτουργικού πλαισίου που αποτελείται από τέσσερις φάσεις, οι οποίες είναι Αναγνώριση απειλών και επιθέσεων, Ανακάλυψη υφιστάμενης επίγνωσης, δημιουργία προσέγγισης συνειδητοποίησης και αξιολόγηση προσέγγισης επίγνωσης. Τα αποτελέσματα της έρευνας αυτής οδήγησαν σε μια προσέγγιση ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο, ειδικά για την ηλικιακή ομάδα k-12, η οποία αξιοποιεί τα emoji για την

ασφάλεια στον κυβερνοχώρο. Έτσι, μέσα από τα αποτελέσματα της έρευνας αυτής έχει φανεί ότι η κοινότητα ασφαλείας μπορεί να εγγράψει και να παρασύρει τους εφήβους στην ασφάλεια στον κυβερνοχώρο και να αυξήσει τον βαθμό ευαισθητοποίησης σχετικά με την ασφάλεια [31].

Επιπρόσθετα, η έρευνα των Muniandi et al., είχε σκοπό να διερευνήσει την τρέχουσα κατάσταση της συμπεριφοράς για ασφάλεια στον κυβερνοχώρο μεταξύ των μαθητών δευτεροβάθμιας εκπαίδευσης στη Μαλαισία. Η συμπεριφορά των ερωτηθέντων για την ασφάλεια στον κυβερνοχώρο αξιολογήθηκε στις ακόλουθες πτυχές: χρήση κωδικού πρόσβασης, phishing, διαδικτυακή απάτη και κακόβουλο λογισμικό. Το μέσο συλλογής δεδομένων της έρευνας αυτής ήταν το ερωτηματολόγιο το οποίο δόθηκε σε φοιτητές σε ένα καλά εδραιωμένο πανεπιστημιακό κολέγιο που βρίσκεται στη βόρεια περιοχή της χερσονήσου της Μαλαισίας. Τα αποτελέσματα της έρευνας αυτής έχουν δείξει ότι η συμπεριφορά στον κυβερνοχώρο μεταξύ των ερωτηθέντων ήταν γενικά μη ικανοποιητική και στα πέντε ζητήματα ασφάλειας στον κυβερνοχώρο που είχαν μελετηθεί σε αυτήν την έρευνα. Συνεπώς πρέπει να παρέχεται εκπαίδευση για τη βέλτιστη πρακτική στο διαδίκτυο [2].

Επιπρόσθετα, στην έρευνα του Bustard, ο σκοπός ήταν να εξεταστεί το πώς μπορεί να βελτιωθεί η δέσμευση των μαθητών στην μελέτη της ασφάλειας του κυβερνοχώρου. Στην έρευνα αυτή προσδιορίστηκαν 4 κατευθυντήριες αρχές για την προώθηση της δέσμευσης αυτής: (1) ευθυγράμμιση του διδακτικού περιεχομένου με τα ενδιαφέροντα των μαθητών, (2) λαμβάνοντας μια ρεαλιστική και όχι μια φιλοσοφική προσέγγιση για την επίλυση ζητημάτων, (3) αντιμετώπιση της πλήρους πολυπλοκότητας των πραγματικών περιπτωσιολογικών μελετών και (4) κάλυψη περιεχομένου με τρόπο που οι μαθητές βρίσκουν διασκεδαστικό. Μια σημαντική πτυχή του σχεδιασμού που προκύπτει είναι ότι ενθαρρύνει τους μαθητές να δουν τα ηθικά ζητήματα με συστημικούς όρους και όχι από ατομική προοπτική, με ζητήματα που προκύπτουν από μια σύγκρουση μεταξύ διαφορετικών ομάδων με διαφορετικά κατοχυρωμένα συμφέροντα [32].

Ακόμα, μια άλλη έρευνα, αυτή των Jethwani et al., έχει χρησιμοποιήσει ποιοτικά δεδομένα που συγκεντρώθηκαν από ομάδες εστίασης με έφηβα κορίτσια που συμμετείχαν σε ένα καλοκαιρινό πρόγραμμα κυβερνοασφάλειας. Το δείγμα της έρευνας αυτής αποτελείτο από 38 έφηβα κορίτσια. Μέσα από την μελέτη αυτή έγινε προσπάθεια να εξεταστεί το πώς αντιλαμβάνονται τα κορίτσια το πεδίο της κυβερνοασφάλειας καθώς επίσης και ποιες είναι οι υποσχόμενες πρακτικές οι οποίες εμπλέκουν τα κορίτσια στην εκπαίδευση στον κυβερνοχώρο. Τα αποτελέσματα της έρευνας αυτής έχουν δείξει ότι οι συνεργατικές

σκηνές ενός φύλου με ενθαρρυντικούς και υποστηρικτικούς εκπαιδευτές συμβάλλουν στο αυξημένο ενδιαφέρον των παιδιών στον τομέα της κυβερνοασφάλειας. Μέσα από τα αποτελέσματα της έρευνας αυτής, έχει φανεί ότι η έμφαση στις δημιουργικές και συνεργατικές διαδικασίες επίλυσης προβλημάτων και στην εφαρμογή του πραγματικού κόσμου που είναι εγγενής στην ασφάλεια στον κυβερνοχώρο είναι πιθανό να αυξήσει τη συμμετοχή των κοριτσιών στο πεδίο της ασφάλειας στον κυβερνοχώρο. Τα αποτελέσματα έχουν επιπτώσεις για τους εκπαιδευτικούς, τους ερευνητές και τους υπεύθυνους χάραξης πολιτικής που στοχεύουν να κλείσουν τα χάσματα μεταξύ των φύλων στον τομέα της επιστήμης των υπολογιστών και να αναπτύξουν ενδιαφέρον για την ασφάλεια στον κυβερνοχώρο, έναν τομέα κρίσιμης εθνικής ανάγκης [33].

Α/Α	Συγγραφέας	Σκοπός	Δείγμα	Μέσο-Μέθοδος	Αποτελέσματα
1	Jin et al. 2018	GenCyber για τόνωση του ενδιαφέροντος των μαθητών K-12 στην κυβερνοασφάλεια και να αυξηθεί η ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο	181 μαθητές γυμνασίου	Εφαρμογή δραστηριοτήτων στο παιχνίδι, Παρακολούθηση	η μάθηση μέσω αυτών των δραστηριοτήτων έχει αποδειχθεί πολύ αποτελεσματική στην εκπαίδευση ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο
2	Jones et al., 2017	Να προσδιοριστούν οι γνώσεις οι δεξιότητες και οι ικανότητες που πρέπει να συμπεριλαμβάνονται στην εκπαίδευση και κατάρτιση στον κυβερνοχώρο	44 επαγγελματίες ασφάλειας	συνέντευξη	Πρέπει να δίνεται έμφαση στην απόκτηση γνώσεων, δεξιοτήτων και ικανοτήτων που αφορούν τα δίκτυα κατά την εκπαίδευση στα σχολεία.
3	Muniandi et al., 2017	Να διερευνήσει την τρέχουσα κατάσταση της συμπεριφοράς για ασφάλεια στον κυβερνοχώρο μεταξύ των μαθητών δευτεροβάθμιας εκπαίδευσης στη Μαλαισία.		ερωτηματολόγιο	Πρέπει να παρέχεται εκπαίδευση για τη βέλτιστη πρακτική στο διαδίκτυο
4	Al-Tajer et al., 2022	να αναπτυχθεί ένα πλαίσιο που αντιμετωπίζει την έλλειψη ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο για τους μαθητές γυμνασίου.		Πρόταση πλαισίου για την παροχή αποτελεσματικών προσεγγίσεων ευαισθητοποίησης για το k12	Η κοινότητα ασφαλείας μπορεί να εγγράψει και να παρασύρει τους εφήβους στην ασφάλεια στον κυβερνοχώρο και να αυξήσει τον βαθμό ευαισθητοποίησης σχετικά με την ασφάλεια
5	Al-Janabi et al., 2016	Να αναλύσει την ευαισθητοποίηση για την ασφάλεια των πληροφοριών μεταξύ του ακαδημαϊκού προσωπικού, ερευνητών, προπτυχιακών φοιτητών και εργαζομένων σε εκπαιδευτικά περιβάλλοντα.			Οι συμμετέχοντες δεν είχαν την απαιτούμενη γνώση και κατανόηση της σημασίας της ασφάλειας πληροφοριών και της πρακτικής εφαρμογής τους στην καθημερινή τους εργασία. Αυτή η κατάσταση μπορεί να διορθωθεί μέσω ολοκληρωμένων προγραμμάτων ευαισθητοποίησης και κατάρτισης.

6	Chou et al., 2016	Να διερευνηθούν οι παράγοντες που σχετίζονται με τη συμπεριφορά των εκπαιδευτικών στην ασφάλεια των πληροφοριών, όπως βασίζεται στη Θεωρία Κίνητρων Προστασίας.	505 συμμετέχοντες	αναπτύχθηκε μια κλίμακα για τη μέτρηση των αντιλήψεων των εκπαιδευτικών για τα κίνητρα προστασίας και την προβληματική συμπεριφορά InfoSec	Εξήχθησαν πέντε παράγοντες: η αντιληπτή σοβαρότητα, η αντιληπτή ευαλωτότητα, η αποτελεσματικότητα απόκρισης, το κόστος απόκρισης και η αυτοαποτελεσματικότητα.
7	Javidi et al., 2018	Να γίνει προώθηση ερευνητικών ατζεντών σχετικά με την κυβερνοασφάλεια και να εκπαιδευτεί η μελλοντική γενιά σε θέματα δεξιοτήτων στην κυβερνοασφάλεια.			Η εκπαίδευση στην κυβερνοασφάλεια αποτελεί ένα νέο μοντέλο εκπαίδευσης
8	Haseski 2020	Να προσδιορίσει την επίδραση των ατομικών δεξιοτήτων ασφάλειας στον κυβερνοχώρο των εκπαιδευτικών και τη στάση τους απέναντι στην εκπαίδευση με τη βοήθεια υπολογιστή.	241 καθηγητές	"Προσωπική Κλίμακα Παροχής Ασφάλειας στον Κυβερνοχώρο" "Η Κλίμακα Στάσης προς την Εκπαίδευση Υποβοηθούμενη από Υπολογιστή".	Υπήρχαν διαφορές μεταξύ των προσωπικών βαθμολογιών ασφάλειας στον κυβερνοχώρο των εκπαιδευτικών
9	Corrandini et al., (2020)	Η διερεύνηση των αντιλήψεων των εκπαιδευτικών σε σχολεία της Ιταλίας για την ψηφιακή επίγνωση των μαθητών τους και την αξιολόγησή τους για τις ενέργειες που απαιτούνται για την ανάπτυξή της.	μέρος 2.229 εκπαιδευτικοί	εθνικό πρόγραμμα	Υψηλή ευαισθησία των εκπαιδευτικών σε θέματα ψηφιακής ευαισθητοποίησης. Ανάγκη εκπαίδευσης για την ψηφιακή ευαισθητοποίηση
10	Caparino 2018	Διερεύνηση των αντιλήψεων για την ασφάλεια στον κυβερνοχώρο μεταξύ των εκπαιδευτικών	84 εκπαιδευτικοί	ερωτηματολόγιο	Ανάπτυξη προγραμμάτων για την ασφάλεια στον κυβερνοχώρο μεταξύ των εκπαιδευτικών

11	Chen et al., 2016	να περιγράψει πώς πολλά σχολικά ιδρύματα αντιμετώπιζαν την απώλεια εμπιστευτικών πληροφοριών και προστατεύοντας τους μαθητές στο WWW, το καθένα μέσα από ένα μοναδικό σύνολο περιστάσεων		προσέγγιση μελέτης περίπτωσης	Με τις εμπειρίες, οι σχολικές περιφέρειες είναι σημαντικό λαμβάνουν μέτρα για να προσφέρουν εκπαίδευση αξίας βελτιώνοντας τις γνώσεις και την επίγνωση των μαθητών σχετικά με τις έννοιες της Κυβερνοηθικής και της Κυβερνοασφάλειας
12	Chen et al., 2019	Να περιγραφεί το ζήτημα της κυβερνοηθικής, της κυβερνοασφάλειας και της ασφάλειας στον κυβερνοχώρο (3Cs), καθώς και πώς τα προβλήματα αυτών των τριών αναμειγνύονται για να γίνουν γενικά ζητήματα κυβερνοηθικής για την κοινωνία.		μελέτη περίπτωσης	Μέσα από την έρευνα αυτή προωθούνται οι καλοί κυβερνοπολίτες στα σχολεία επειδή είναι πολύ σημαντικό για τις σχολικές περιφέρειες να λάβουν ορισμένα μέτρα για τη βελτίωση της γνώσης και της ευαισθητοποίησης των μαθητών σχετικά με την κυβερνοηθική, την ασφάλεια στον κυβερνοχώρο.
13	Bustard 2018	Να εξεταστεί το πώς μπορεί να βελτιωθεί η δέσμευση των μαθητών στην μελέτη της ασφάλειας του κυβερνοχώρου		Μελέτη περίπτωσης	Μια σημαντική πτυχή του σχεδιασμού που προκύπτει είναι ότι ενθαρρύνει τους μαθητές να δουν τα ηθικά ζητήματα με συστημικούς όρους και όχι από ατομική προοπτική.
14	Jethwani et al., 2017	να εξεταστεί το πώς αντιλαμβάνονται τα κορίτσια το πεδίο της κυβερνοασφάλειας καθώς επίσης και ποιες είναι οι υποσχόμενες πρακτικές οι οποίες εμπλέκουν τα κορίτσια στην εκπαίδευση στον κυβερνοχώρο	38 έφηβα κορίτσια	Ποιοτική μελέτη	Τα αποτελέσματα της έρευνας αυτής έχουν δείξει ότι οι συνεργατικές σκηνές ενός φύλου με ενθαρρυντικούς και υποστηρικτικούς εκπαιδευτές συμβάλλουν στο αυξημένο ενδιαφέρον των παιδιών στον τομέα της κυβερνοασφάλειας.
15	Olano et al., 2014	Να δημιουργηθεί ένα παιχνίδι το οποίο ευαισθητοποιεί τους μαθητές σχετικά με τις πρακτικές ασφάλειας στον κυβερνοχώρο.	Παιδιά ηλικίας K-12	Εφαρμογή δραστηριοτήτων στο παιχνίδι, Παρακολούθηση	Το παιχνίδι είναι ελκυστικό και αυξάνει την ευαισθητοποίηση σχετικά με τις πρακτικές ασφάλειας στον κυβερνοχώρο.

16	Lendezci et al., 2019	Να αναπτυχθεί ένα ρομπότ το οποίο κάνει τις βασικές ιδέες στην επιστήμη των υπολογιστών προσιτές σε ομάδες μαθητών K-12 να ευαισθητοποιούνται στην ασφάλεια στον κυβερνοχώρο	24 μαθητές K-12	Εφαρμογή δραστηριοτήτων στο παιχνίδι RoboScape, Παρακολούθηση	Ασφάλεια στον κυβερνοχώρο αποτελεί άμεση ανάγκη που οι μαθητές αντιλαμβάνονται και μπορούν να εργαστούν για να αντιμετωπίσουν.

Πίνακας 1: Ανασκόπηση Βιβλιογραφίας

Κεφάλαιο 3
Μεθοδολογία

3.1 Περίληψη

Σε αυτό το κεφάλαιο, γίνεται προσπάθεια για εντοπισμό των στοιχείων εκείνων που χρησιμοποιούνται για την επίλυση των ερευνητικών προβλημάτων που έχουν τεθεί στην αρχή της παρούσας μελέτης. Παρουσιάζονται, λοιπόν, οι έννοιες και οι λειτουργικοί ορισμοί που χρησιμοποιούνται στην έρευνα, περιγράφονται οι κλίμακες μέτρησης των μεταβλητών του ερωτηματολογίου, αναφέρεται βαθμός αξιοπιστίας και εγκυρότητας των μετρήσεων και τέλος καθορίζεται ο πληθυσμός και το μέσο συλλογής δεδομένων. Για τη μεθοδολογία της έρευνας το μέσο συλλογής δεδομένων που έχει χρησιμοποιηθεί είναι το ερωτηματολόγιο το οποίο έχει σταλεί σε ηλεκτρονική μορφή σε 100 εκπαιδευτές των κλάδων ηλεκτρολογίας και μηχανικής ηλεκτρονικών υπολογιστών των τεχνικών σχολών Κύπρου. Τα ερωτηματολόγια στάλθηκαν σε ηλεκτρονική μορφή σε όλες τις τεχνικές σχολές της Κύπρου. Στη συνέχεια, η επεξεργασία των αποτελεσμάτων έχει γίνει με το στατιστικό πρόγραμμα SPSS23.

3.2 Φιλοσοφικό Πλαίσιο

3.2.1 Είδος Έρευνας

Το είδος της έρευνας που χρησιμοποιείται στην παρούσα μεταπτυχιακή εργασία είναι η ποσοτική έρευνα. Ο τύπος της ποσοτικής έρευνας ασχολείται με τη συλλογή δεδομένων χρησιμοποιώντας διάφορα μέσα όπως είναι το ερωτηματολόγιο. Χρησιμοποιήθηκε αυτός ο τύπος έρευνας λόγω του ότι βοηθά στη μέτρηση των αποτελεσμάτων και έτσι μπορεί να γίνει πιο εύκολη η ανάλυση και η εξαγωγή των αποτελεσμάτων.

Γενικότερα, υπάρχουν διάφορα είδη έρευνας. Κάθε ένα από αυτά χρησιμοποιείται και για κάποιο σκοπό. Τα είδη αυτά ταξινομούνται ανάλογα με το σκοπό για τον οποίο είναι δημιουργημένα. Για παράδειγμα μπορούμε να έχουμε έρευνες ερωτηματολογίου, συνέντευξης, παρατήρησης και σταθμισμένου τεστ, κλπ. Επιπρόσθετα, μπορούν να ταξινομηθούν ανάλογα με το σκοπό της κάθε έρευνας: (1) Βασική έρευνα, η οποία παρουσιάζει απλά νέα πράγματα χωρίς όμως να δημιουργεί το αποτέλεσμα. (2) Εφαρμοσμένη έρευνα, η οποία εστιάζει περισσότερο στο πρακτικό κομμάτι [2].

Επιπλέον, μπορούν να ταξινομηθούν ανάλογα με την κατηγορία της κάθε έρευνας: (1) Ποιοτική έρευνα, η οποία μελετά ξεχωριστά την κάθε περίπτωση, (2) Ποσοτική έρευνα, η οποία συλλέγει τα δεδομένα χρησιμοποιώντας κάποια μέσα συλλογής δεδομένων που είναι συνήθως τα ερωτηματολόγια και στη συνέχεια προχωρά στην ανάλυση των ευρημάτων.

Ακολουθώντας το κεφάλαιο Βιβλιογραφική Ανασκόπηση, το κεφάλαιο Μεθοδολογία είναι το βασικό κεφάλαιο για την έρευνα. Με την επιλογή του θέματος, περιγράφεται χρονικά η πορεία και τα στάδια που ακολουθήθηκαν για τη διεξαγωγή της έρευνας. Κατά τη διαδικασία αυτή ετοιμάζεται το ερωτηματολόγιο το οποίο επρόκειτο να δοθεί σε 100 εκπαιδευτικούς Μέσης Τεχνικής Εκπαίδευσης σε όλη την Κύπρο.

Προτού μοιραστούν τα ερωτηματολόγια στους εκπαιδευτικούς, ήταν αναγκαίο να παρουσιαστεί ο σκοπός για τον οποίο έχει γίνει η έρευνα αυτή. Έπειτα, μετά από αποστολή του ερωτηματολογίου στα ηλεκτρονικά ταχυδρομεία των Τεχνικών Σχολών της Κύπρου, αναμενόταν να συμπληρωθούν 100 συνολικά ερωτηματολόγια. Θα πρέπει να τονιστεί ότι οι ερωτηθέντες παρέμειναν ανώνυμοι κατά την έρευνα αυτή και να προτρέπονταν να απαντήσουν με συνέπεια και με ειλικρίνεια σε όλες τις ερωτήσεις τους ερωτηματολογίου. Αφού ολοκληρώθηκε η διαδικασία απαντήσεων, η ηλεκτρονική έρευνα έκλεισε και ακολούθησε η επεξεργασία των δεδομένων για την εξαγωγή των αποτελεσμάτων.

3.3 Μέσο Συλλογής Δεδομένων

Το ερωτηματολόγιο ήταν το μοναδικό μέσο συλλογής δεδομένων που χρησιμοποιήθηκε στην παρούσα μεταπτυχιακή εργασία. Σκοπός της δημιουργίας ερωτηματολογίου ήταν να συλλεχθούν οι απόψεις και οι στάσεις των εκπαιδευτικών Μέσης Τεχνικής Εκπαίδευσης των κλάδων Μηχανικής Ηλεκτρονικών Υπολογιστών και Ηλεκτρολογίας σχετικά με την εφαρμογή της ασφάλειας στον Κυβερνοχώρο ως μάθημα στα σχολεία Μέσης Τεχνικής Εκπαίδευσης.

Το ερωτηματολόγιο αποτελείτο από δύο μέρη. Στο πρώτο μέρος, τα δημογραφικά στοιχεία, περιλαμβάνονταν έξι ερωτήσεις σχετικές με τα δημογραφικά στοιχεία των εκπαιδευτικών όπως είναι το φύλο τους, η ηλικία, οργανική θέση, ειδικότητα, εκπαίδευση καθώς και εμπειρία. Στο δεύτερο μέρος, το κυρίως μέρος, περιλαμβάνονταν 18 ερωτήματα σχετικά με τη στάση και τις απόψεις των εκπαιδευτικών ως προς την διδασκαλία της κυβερνοασφάλειας στα σχολεία, 5 ερωτήματα σχετικά με τους τρόπους που μπορεί να προσφερθεί το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική

Εκπαίδευση και 3 ερωτήσεις σχετικά με τα προβλήματα που θα μπορούσε να έχει ή όχι η εφαρμογή ενός τέτοιου μαθήματος στα σχολεία Μέσης Τεχνικής Εκπαίδευσης.
Είναι πολύ βασικό να ακολουθούνται κάποιες πρακτικές ώστε να χειρίζεται η χρήση ευαίσθητων δεδομένων των ερωτηθέντων.
Ήταν επίσης πολύ σημαντικό να καταγραφεί ο χρόνος ο οποίος χρειάζεται για τη συμπλήρωση του ερωτηματολογίου. Οπότε, προτού σταλούν τα ερωτηματολόγια, η ερευνήτρια συμπλήρωσε ένα δοκιμαστικό ερωτηματολόγιο για να υπολογιστεί ένα περίπου ο μέσος χρόνος που χρειάζεται ένας εκπαιδευτικός για να το συμπληρώσει. Το γεγονός αυτό βοηθάει σε μια αξιόπιστη συλλογή δεδομένων.

3.3.1 Είδη Δεδομένων

Οι 100 εκπαιδευτικοί Μέσης Τεχνικής Εκπαίδευσης ήταν τα άτομα τα οποία έλαβαν μέρος στη συμπλήρωση του ερωτηματολογίου. Οι εκπαιδευτικοί αυτοί κλήθηκαν να συμπληρώσουν το ερωτηματολόγιο το οποίο περιγράφηκε στην προηγούμενη παράγραφο.
Μέσα από τη δομή του ερωτηματολογίου περιγράφονται και οι μεταβλητές του. Ανεξάρτητες μεταβλητές θεωρούνται (α) οι εκπαιδευτικοί και (β) η διδασκαλία της κυβερνοασφάλειας στα σχολεία Μέσης Τεχνικής Εκπαίδευσης.
Εξαρτημένη μεταβλητή είναι οι απόψεις και στάσεις των εκπαιδευτικών για τη διδασκαλία της κυβερνοσφάλειας στα σχολεία Μέσης Τεχνικής Εκπαίδευσης.

3.4 Καθορισμός Πληθυσμού – Δείγμα

Η υποενότητα αυτή παρουσιάζει τον Πληθυσμό-δείγμα της έρευνας. Ο πληθυσμός της έρευνας είναι 100 εκπαιδευτικοί Μέσης Τεχνικής Εκπαίδευσης οι οποίοι υπάγονται στον κλάδο Μηχανικής Ηλεκτρονικών Υπολογιστών ή Ηλεκτρολογίας από όλες τις επαρχίες της Κύπρου κατά τη σχολική χρονιά 2022-2023.
Μετά τον καθορισμό του δείγματος της παρούσα έρευνας, ήταν αναγκαίο να γίνει και ο καθορισμός του τρόπου επιλογής των ερωτηθέντων. Αποφασίστηκε ότι η δειγματοληψία θα είναι η δειγματοληψία ευκολίας. Δηλαδή, ήδη ήταν επιλεγμένα τα σχολεία και οι εκπαιδευτικοί θα συμπλήρωναν τα ερωτηματολόγια μέχρι να γίνουν 100 στο σύνολο.
Έχει επιλεγεί η δειγματοληψία αυτή λόγω του ότι είναι εύκολη στην επιλογή του δείγματος.

3.5 Παραδοχές της Έρευνας

Η παραδοχή είναι μια προϋπόθεση η οποία τίθεται από κάποιο ερευνητή ώστε να ισχύει μια συνθήκη και να μην μπορεί να προχωρήσει η έρευνα χωρίς τη συγκεκριμένη συνθήκη [2].

Η πρώτη παραδοχή εδώ σε αυτή την έρευνα είναι ότι οι εκπαιδευτικοί ανήκουν στην Μέση Τεχνική Εκπαίδευση. Μια άλλη παραδοχή είναι το γεγονός ότι οι εκπαιδευτικοί υπάγονται στον κλάδο Μηχανικής Ηλεκτρονικών Υπολογιστών ή Ηλεκτρολογίας. Τέλος μια άλλη παραδοχή είναι το γεγονός ότι οι εκπαιδευτικοί γνωρίζουν γενικά για την ασφάλεια.

3.6 Στατιστικές Τεχνικές

Η ανάλυση των δεδομένων στην παρούσα έρευνα έχει γίνει με τη χρήση του στατιστικού προγράμματος SPSS23. Σύμφωνα με τα αποτελέσματα των ερωτήσεων, έχει υπολογιστεί η συχνότητα (frequency) μέτρησης της κάθε ερώτησης και έχουν εξαχθεί τα ανάλογα αποτελέσματα. Επίσης γίνεται συσχέτιση (crosstabs) των δημογραφικών στοιχείων με ερωτήματα από το δεύτερο μέρος του ερωτηματολογίου.

Μετά τη συλλογή των ερωτηματολογίων, έπρεπε να κωδικοποιηθεί ένα ερωτηματολόγιο με τις ερωτήσεις του ερωτηματολογίου για να μας βοηθήσει να περάσουμε εύκολα τα δεδομένα του ερωτηματολογίου στο πρόγραμμα. Αυτή η φόρμα είναι ένας πίνακας που κωδικοποιεί τις ερωτήσεις από το ερωτηματολόγιο. Η πρώτη στήλη του πίνακα καταγράφει τους αριθμούς των ερωτήσεων όπως εισήχθησαν στο λογιστικό πρόγραμμα, η δεύτερη στήλη παραθέτει τις περιγραφές των μεταβλητών και τις ετικέτες που χρησιμοποιούνται στο πρόγραμμα και η τρίτη στήλη τους κωδικούς απαντήσεων. Η πρώτη ερώτηση, για παράδειγμα, ζητά από τους συμμετέχοντες να σημειώσουν το φύλο τους και έχει δύο πιθανές απαντήσεις: 1 για τον άνδρα και 2 για τη γυναίκα. Εάν ο συμμετέχων δεν απαντήσει σε αυτήν την ερώτηση, τότε η κωδικοποίηση θα λάβει την τιμή 0 που αντιστοιχεί στην τιμή "Δεν απάντησε".

Στη συνέχεια, τα δεδομένα των ερωτηματολογίων έχουν περάσει μέσω της κωδικοποίησής τους στο στατιστικό πρόγραμμα. Επίσης, για να γίνει σωστή επαλήθευση των στοιχείων, τα ερωτηματολόγια αριθμήθηκαν και επαληθεύτηκαν μετά την καταχώρισή τους. Αυτό απέφυγε τα σφάλματα εισαγωγής δεδομένων.

3.7 Κανόνες δεοντολογίας και ηθικής

Η συλλογή των δεδομένων έγινε με τη χρήση του ερωτηματολογίου. Οι επιλεγμένοι συμμετέχοντες κλήθηκαν να απαντήσουν με συνέπεια σε όλες τις ερωτήσεις πολλαπλής επιλογής του ερωτηματολογίου που τους δόθηκε. Ωστόσο, ως έρευνα, πρέπει να λαμβάνει υπόψη κανόνες δεοντολογίας που βοηθούν στην εξαγωγή αποτελεσμάτων χωρίς σφάλματα.

Στο βιβλίο Εκπαιδευτική Έρευνα Παπαναστασίου & Παπαναστασίου (2005), τονίζονται οι ακόλουθοι κανόνες ηθικής:

• Κανείς δεν αναγκάζεται να λάβει μέρος στην έρευνα.

• Σκοπός αυτής της έρευνας είναι να φέρει στην κοινωνία αποτελέσματα που είναι ωφέλιμα.

• Οι συμμετέχοντες στην έρευνα προστατεύονται από κάθε κίνδυνο.

• Τα προσωπικά στοιχεία των ερωτηθέντων που συλλέγονται για τους σκοπούς της παρούσας έρευνας είναι εμπιστευτικά και προστατεύονται από το νόμο.

• Οι συμμετέχοντες στην έρευνα δεν πρέπει να παραπλανηθούν.

• Τα δεδομένα που συλλέγονται από αυτήν την έρευνα δεν θα υπόκεινται σε καμία αλλαγή.

• Ο ερευνητής δεν θα χρησιμοποιήσει δεδομένα ή αποτελέσματα από άλλη έρευνα, εκτός εάν τοποθετήσει στη βιβλιογραφία του την πηγή που πήρε αυτά τα δεδομένα.

• Οι συμμετέχοντες στην έρευνα θα πρέπει να παρέχουν αληθινές απαντήσεις και πληροφορίες για να βοηθήσουν στην εξαγωγή έγκυρων αποτελεσμάτων.

3.8 Εγκυρότητα και Αξιοπιστία Μετρήσεων

Σύμφωνα με τους Παπαναστασίου & Παπαναστασίου (2005), η εγκυρότητα είναι ο βαθμός που μπορεί ο σκοπός μιας έρευνας. Υπάρχουν κάποια όργανα μέτρησης για τα αποτελέσματα τα οποία δίνουν αποτελέσματα έγκυρα για την έρευνα. Στην παρούσα μελέτη ήταν αναγκαίος ο έλεγχος της εγκυρότητας που δίνουν τα όργανα που χρησιμοποιούνται για τη μέτρηση των αποτελεσμάτων.

Γενικότερα υπάρχουν τέσσερις τύποι εγκυρότητας: (1) Φαινομενική εγκυρότητα, δηλαδή ο βαθμός μέτρησης ενός οργάνου που δίνει το μέσο όρο των απαντήσεων μιας ερώτησης, (2) Εγκυρότητα περιεχομένου, δηλαδή ο βαθμός εγκυρότητας που βασίζεται στη σύγκριση των ερωτήσεων, (3) Εγκυρότητα σχετιζόμενη με κριτήριο, δηλαδή η εγκυρότητα η οποία βασίζεται σε μελλοντικά κριτήρια μιας έρευνας, (4) Εγκυρότητα εννοιολογικής κατασκευής, δηλαδή η εγκυρότητα που ερμηνεύει τα αποτελέσματα ψυχολογικών ιδιοτήτων (Παπαναστασίου & Παπαναστασίου, 2005: 157-163).

Η αξιοπιστία των μετρήσεων, παρουσιάζει το πόσο αξιόπιστο είναι το μέσο συλλογής δεδομένων που χρησιμοποιεί κάποιος ερευνητής. Στη δική μας την περίπτωση, το μέσο συλλογής δεδομένων είναι το ερωτηματολόγιο. Η αξιοπιστία έχει τα ακόλουθα χαρακτηριστικά: (1) εμφανίζεται μόνο στα αποτελέσματα του μέσου συλλογής δεδομένων, (2) είναι αναγκαία σε οποιαδήποτε έρευνα όμως δεν είναι επαρκές στοιχείο για να θεωρείται ότι είναι έγκυρη, (3) η μέτρησή της βασίζεται σε σταθερά δεδομένα, και (4) διαπιστώνεται μέσα από στατιστική ανάλυση. (ό.π.: 163-165)

Στην παρούσα μελέτη, η μέτρηση της αξιοπιστίας με βάση το ερωτηματολόγιο γίνεται με δύο προσεγγίσεις: (α) όταν δύο από τις ερωτήσεις γραφούν με τρεις διαφορετικούς τρόπους. Με την επιστροφή των ερωτηματολογίων βρίσκονται οι τρεις συντελεστές συσχέτισης των ερωτήσεων αυτών και έτσι ο μέσος όρος τους δίνει την αξιοπιστία της έρευνας, (β) μια άλλη προσέγγιση είναι η συμπλήρωση του ερωτηματολογίου από κάποια άτομα σε διαφορετικά χρονικά διαστήματα και η σύγκριση των απαντήσεων τους. Αν οι απαντήσεις συμπίπτουν τότε η αξιοπιστία έχει ψηλό βαθμό.

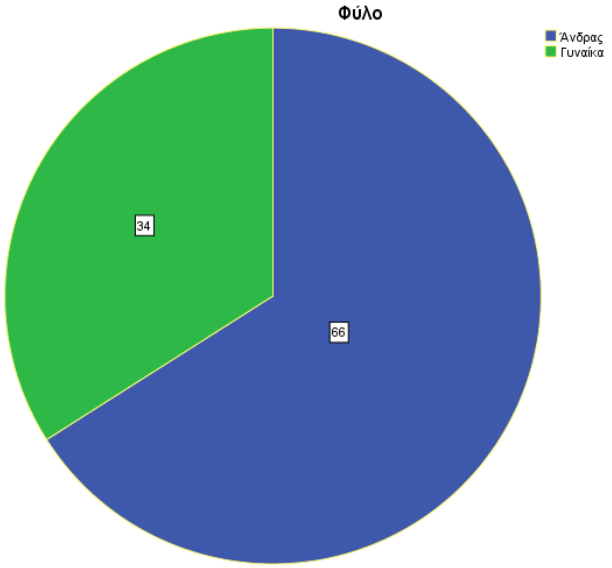
Κεφάλαιο 4
Αποτελέσματα

Εισαγωγή

Στο κεφάλαιο αποτελέσματα παρουσιάζονται τα αποτελέσματα της ανάλυσης των δεδομένων για τους σκοπούς της παρούσας μελέτης. Μέσα από τα αποτελέσματα της παρούσας μελέτης, γίνεται προσπάθεια για να απαντηθούν τα ερευνητικά ερωτήματα τα οποία έχουν τεθεί στην αρχή της μελέτης.

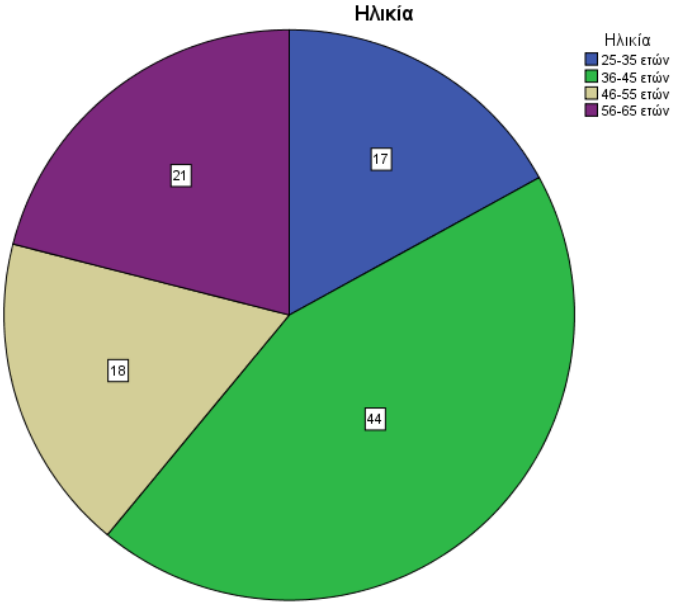
4.1 Δημογραφικά Στοιχεία

Σύμφωνα με τα αποτελέσματα της μελέτης αυτής, και όσον αφορά το φύλο, 66% ήταν άνδρες και 34% γυναίκες (Διάγραμμα 1).



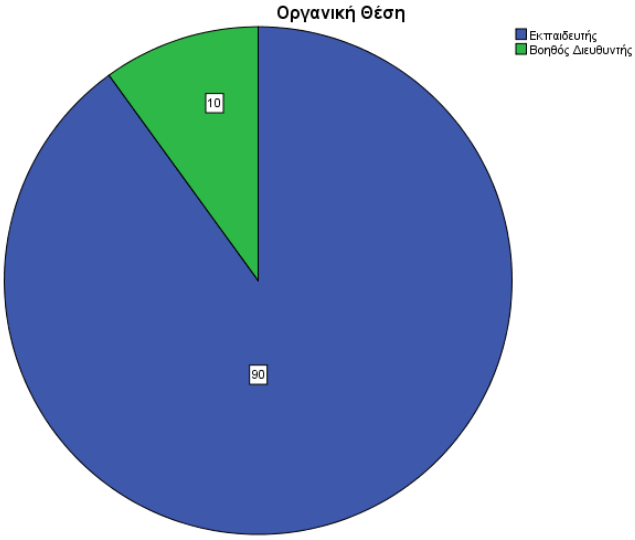
Διάγραμμα 1: Φύλο

Επίσης, όσον αφορά την ηλικία, οι περισσότεροι από τους συμμετέχοντες ανήκαν στην ηλικιακή ομάδα 36-45 ετών (44%). 21% ήταν ηλικίας 56-65 ετών, 18% ήταν ηλικίας 46-55 ετών ενώ 17% ήταν ηλικίας 25-35 ετών (Διάγραμμα 2).



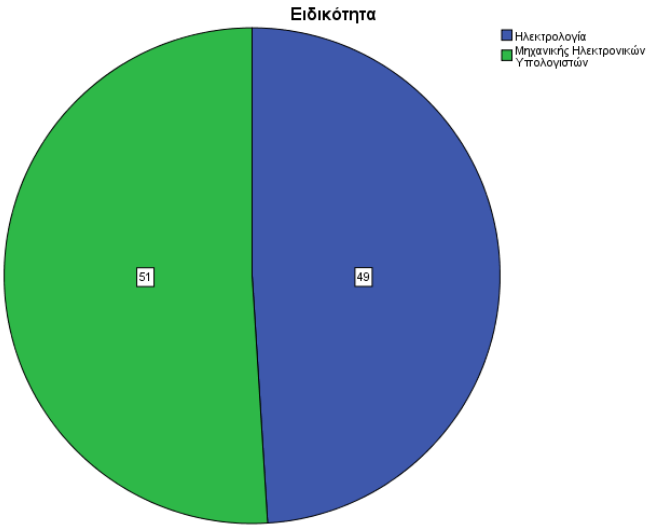
Διάγραμμα 2: Ηλικία

Επιπλέον, 90% από τους συμμετέχοντες ήταν εκπαιδευτές ενώ 10% ήταν Βοηθοί Διευθυντές (Διάγραμμα 3).



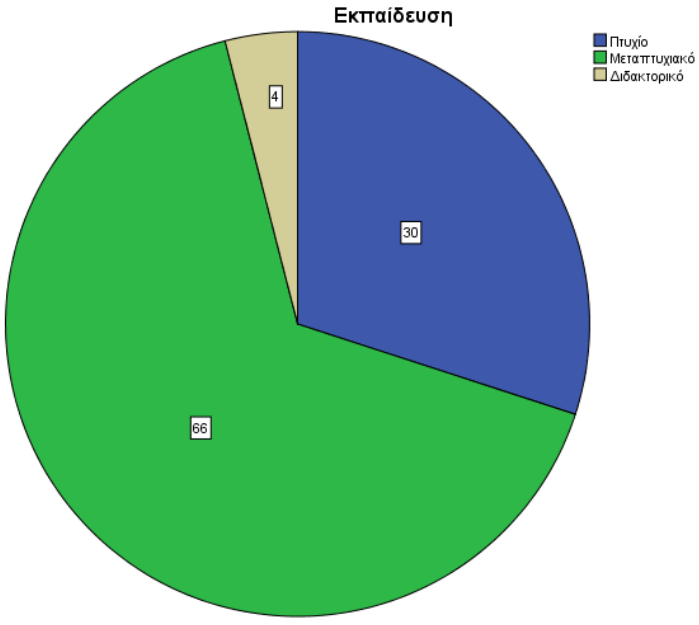
Διάγραμμα 3: Διάγραμμα 3

Επιπρόσθετα, 51% από τους συμμετέχοντες είχαν ειδικότητα Μηχανικής Ηλεκτρονικών Υπολογιστών, ενώ 49% είχαν ειδικότητα Ηλεκτρολογίας (Διάγραμμα 4).



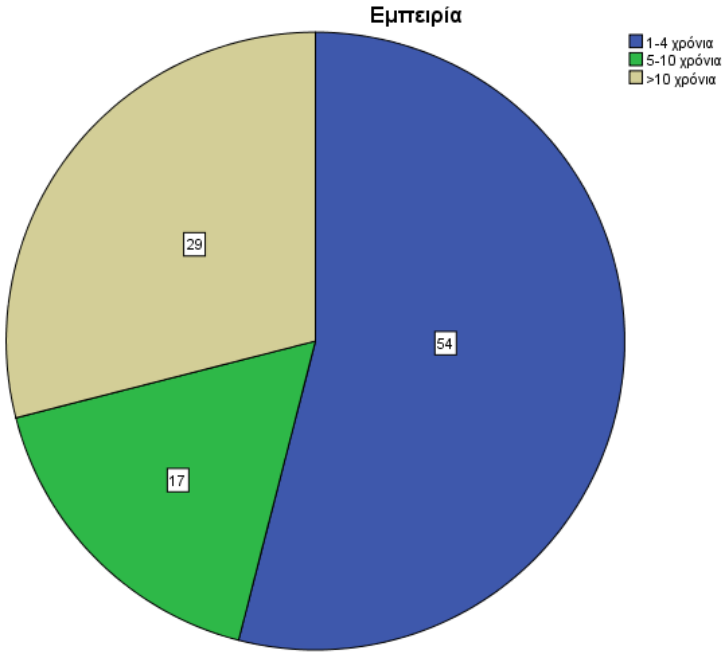
Διάγραμμα 4: Ειδικότητα

Ακόμα, αναφορικά με την εκπαίδευση των συμμετεχόντων, οι περισσότεροι από αυτούς είχαν Μεταπτυχιακό τίτλο (66%). 30% είχαν μόνο πτυχία ενώ 4% είχαν και Διδακτορικό τίτλο (Διάγραμμα 5).



Διάγραμμα 5: Εκπαίδευση

Τέλος, όσον αφορά την εμπειρία, οι περισσότεροι από τους συμμετέχοντες είχαν διδακτική εμπειρία 1-4 χρόνια (54%). 29% είχαν διδακτική εμπειρία περισσότερη από 10 χρόνια ενώ 17% είχαν διδακτική εμπειρία 5-10 χρόνια (Διάγραμμα 6).



Διάγραμμα 6: Εμπειρία

4.2 Κυρίως Έρευνα

4.2.1 Η στάση και οι απόψεις των εκπαιδευτικών ως προς την διδασκαλία της κυβερνοασφάλειας στα σχολεία

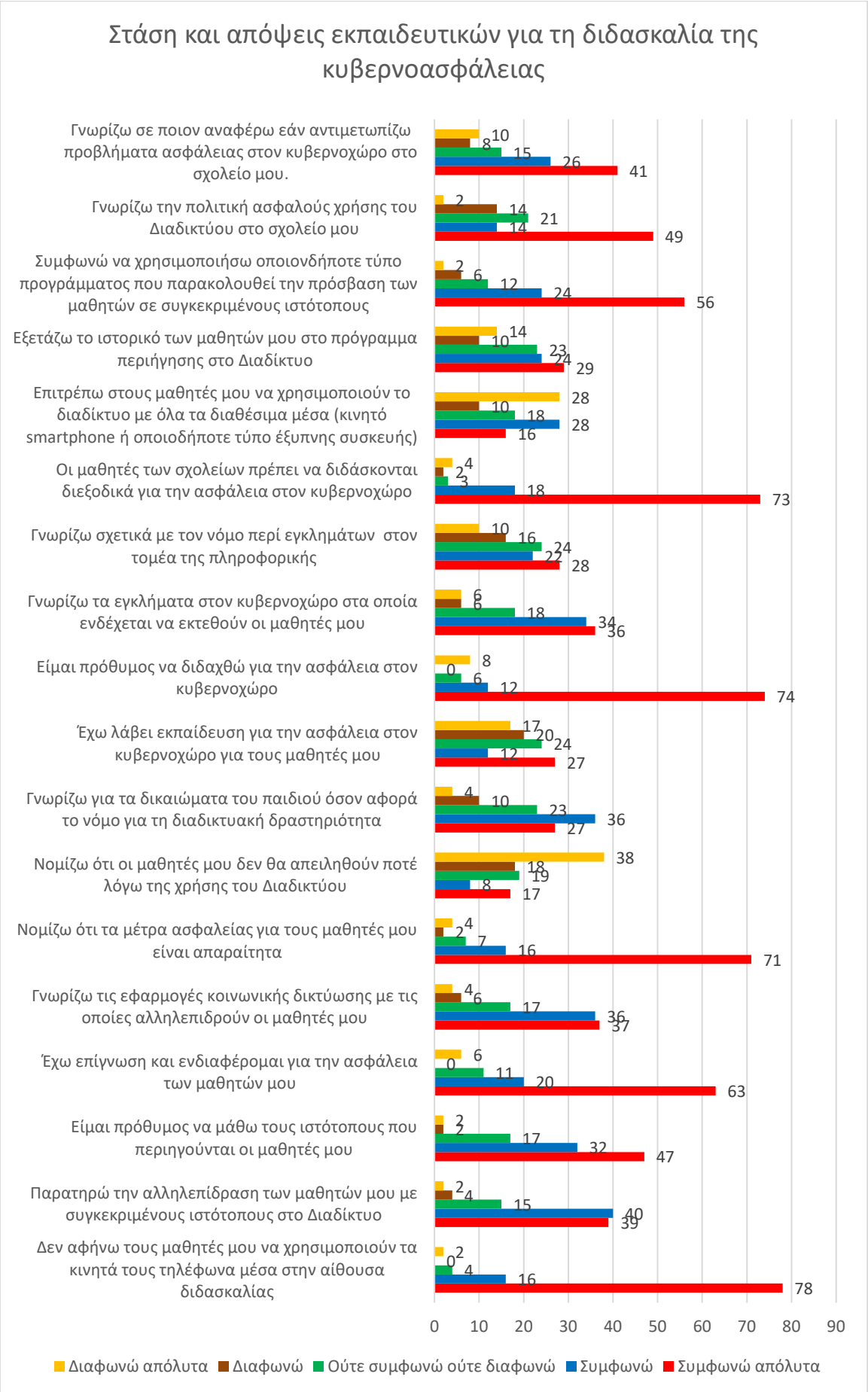
Έχει μελετηθεί η στάση και οι απόψεις των εκπαιδευτικών αναφορικά με τη διδασκαλία της κυβερνοασφάλειας στα σχολεία Μέσης Τεχνικής Εκπαίδευσης.

Στον Πίνακα 2 παρουσιάζονται τα αποτελέσματα σύμφωνα με τις απόψεις των εκπαιδευτικών για τη διδασκαλία της κυβερνοασφάλειας στα σχολεία Μέσης Τεχνικής Εκπαίδευσης. Όπως φαίνεται μέσα από τα αποτελέσματα, οι περισσότεροι από τους εκπαιδευτικούς, συμφωνούν απόλυτα με τις στάσεις ότι, δεν αφήνουν τους μαθητές τους να χρησιμοποιούν τα κινητά τους τηλέφωνα μέσα στην αίθουσα διδασκαλίας (78%), είναι πρόθυμοι να μάθουν τους ιστότοπους που περιηγούνται οι μαθητές τους (47%), έχουν επίγνωση και ενδιαφέρονται για την ασφάλεια των μαθητών τους (63%), γνωρίζουν τις εφαρμογές κοινωνικής δικτύωσης με τις οποίες αλληλεπιδρούν οι μαθητές τους (37%), Νομίζουν ότι τα μέτρα ασφαλείας για τους μαθητές τους είναι απαραίτητα (71%), είναι πρόθυμοι να διδαχθούν για την ασφάλεια στον κυβερνοχώρο (74%), γνωρίζουν τα εγκλήματα στον κυβερνοχώρο στα οποία ενδέχεται να εκτεθούν οι μαθητές τους (36%), γνωρίζουν σχετικά με τον νόμο περί εγκλημάτων στον τομέα της πληροφορικής (28%), συμφωνούν απόλυτα στο γεγονός ότι οι μαθητές των σχολείων πρέπει να διδάσκονται διεξοδικά για την ασφάλεια στον κυβερνοχώρο (73%), εξετάζουν

το ιστορικό των μαθητών τους στο πρόγραμμα περιήγησης στο διαδίκτυο (29%), συμφωνούν να χρησιμοποιήσουν οποιονδήποτε τύπο προγράμματος που παρακολουθεί την πρόσβαση των μαθητών σε συγκεκριμένους ιστότοπους (56%), γνωρίζουν την πολιτική ασφαλούς χρήσης του διαδικτύου στο σχολείο τους (49%) και γνωρίζουν σε ποιον αναφέρονται εάν αντιμετωπίζουν προβλήματα ασφάλειας στον κυβερνοχώρο στο σχολείο τους (41%).

Επίσης, οι περισσότεροι από τους συμμετέχοντες συμφωνούν με τη στάση ότι παρατηρούν την αλληλεπίδραση των μαθητών τους με συγκεκριμένους ιστότοπους στο διαδίκτυο (40%), γνωρίζουν για τα δικαιώματα του παιδιού όσον αφορά το νόμο για τη διαδικτυακή δραστηριότητα (36%), επιτρέπουν στους μαθητές τους να χρησιμοποιούν το διαδίκτυο με όλα τα διαθέσιμα μέσα (κινητό smartphone ή οποιοδήποτε τύπο έξυπνης συσκευής) (28%).

Τέλος, οι περισσότεροι από τους συμμετέχοντες διαφωνούν απόλυτα με τη στάση ότι οι μαθητές τους δεν θα απειληθούν ποτέ λόγω της χρήσης του Διαδικτύου (38%) (Διάγραμμα 7).



Διάγραμμα 7: Στάση και απόψεις εκπαιδευτικών για τη διδασκαλία της κυβερνοασφάλειας

4.2.2 Τρόποι που μπορεί να προσφερθεί το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική Εκπαίδευση

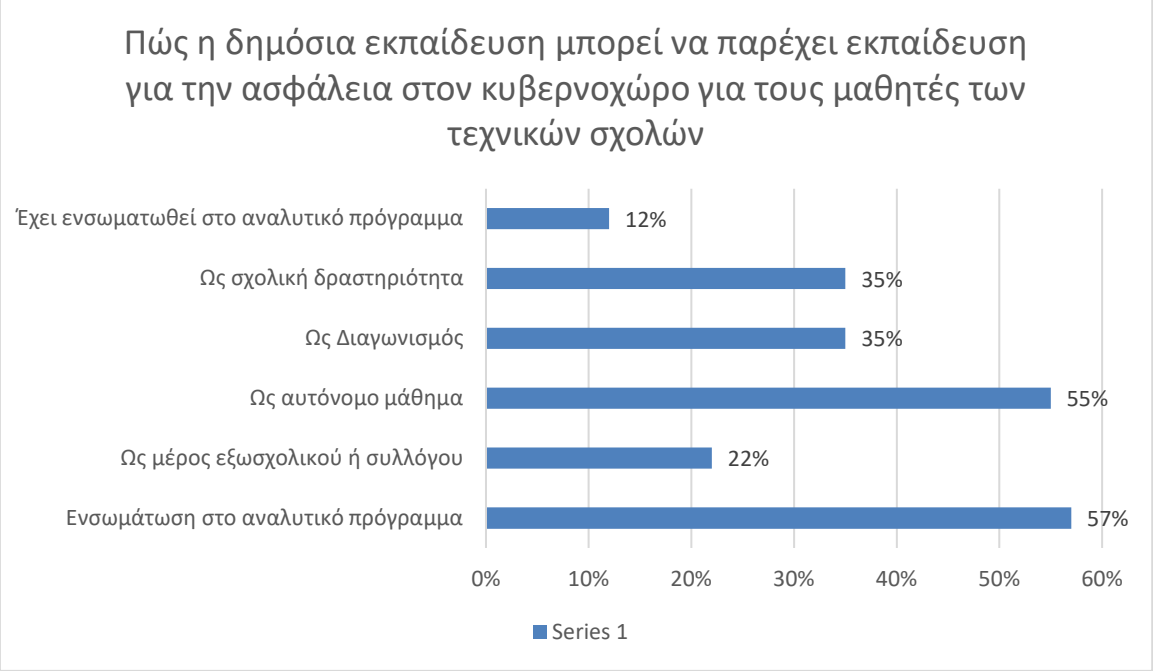
Οι συμμετέχοντες, ερωτήθηκαν αν κατά τη γνώμη τους είναι σημαντικό να προσφέρεται το μάθημα της κυβερνοασφάλειας στη Μέση Τεχνική Εκπαίδευση. Οι περισσότεροι από τους συμμετέχοντες ανέφεραν ότι είναι πολύ σημαντικό (74%) και 26% ότι είναι σημαντικό (Πίνακας 3).

Πίνακας 2

Κατά τη γνώμη σας, είναι σημαντικό να προσφέρεται το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική Εκπαίδευση;

	Συχνότητα	Ποσοστό %
Πολύ σημαντικό	74	74.0
Σημαντικό	26	26.0
Σύνολο	100	100.0

Επίσης, οι συμμετέχοντες ερωτήθηκαν πώς η δημόσια εκπαίδευση μπορεί να παρέχει εκπαίδευση για την ασφάλεια στον κυβερνοχώρο για τους μαθητές των τεχνικών σχολών. Όπως φαίνεται στο Διάγραμμα 7, 57% των συμμετεχόντων προτείνουν ενσωμάτωση στο αναλυτικό πρόγραμμα, 55% προτείνουν να προσφέρεται ως αυτόνομο μάθημα, 35% ως διαγωνισμός και ως σχολική δραστηριότητα, 22% ως μέρος εξωσχολικού ή συλλόγου και 15% ανέφεραν ότι το μάθημα αυτό έχει ήδη ενσωματωθεί στο αναλυτικό πρόγραμμα.



Διάγραμμα 8: πώς η δημόσια εκπαίδευση μπορεί να παρέχει εκπαίδευση για την ασφάλεια στον κυβερνοχώρο για τους μαθητές των τεχνικών σχολών

Επιπλέον, οι συμμετέχοντες κλήθηκαν να αξιολογήσουν το επίπεδο ενδιαφέροντος των μαθητών τους για να μάθουν περισσότερα για την ασφάλεια στον κυβερνοχώρο. Όπως φαίνεται στον πίνακα 9, οι περισσότεροι από τους συμμετέχοντες αξιολόγησαν το επίπεδο ενδιαφέροντος των μαθητών σε υψηλό όσον αφορά τις σχολικές δραστηριότητες (53%) και Διαγωνισμούς (47%) και μέτριο όσον αφορά τα Εξωσχολικά/Σωματεία (40%).

Πίνακας 3: Αξιολόγηση του επίπεδου ενδιαφέροντος των μαθητών να μάθουν περισσότερα για την ασφάλεια στον κυβερνοχώρο

	Χαμηλό		Μέτριο		Υψηλό	
	Σ	%	Σ	%	Σ	%
Εξωσχολικά / Σωματεία	32	32,0	40	40,0	28	28,0
Σχολικές Δραστηριότητες	12	12,0	35	35,0	53	53,0
Διαγωνισμοί	16	16,0	37	37,0	47	47,0

Επιπρόσθετα, οι εκπαιδευτικοί κλήθηκαν να δηλώσουν κατά πόσο θα υπήρχε ενδιαφέρον από τους μαθητές ώστε το μάθημα της κυβερνοασφάλειας να προσφέρεται ως αυτόνομο μάθημα και κατά πόσο θα μπορούσε να ενσωματωθεί στο Αναλυτικό Πρόγραμμα Σπουδών. Σύμφωνα με τις απαντήσεις των συμμετεχόντων, όπως αυτές παρουσιάζονται στον Πίνακα 5, οι περισσότεροι δήλωσαν ότι η κυβερνοασφάλεια μπορεί να προσφερθεί ως αυτόνομο μάθημα με υψηλό ενδιαφέρον (56%) και ότι η κυβερνοασφάλεια μπορεί να ενσωματωθεί στο Αναλυτικό Πρόγραμμα Σπουδών (70%).

Πίνακας 4: Ενδιαφέρον για ενσωμάτωση κυβερνοασφάλειας στο αναλυτικό πρόγραμμα σπουδών και προσφορά της ως αυτόνομο μάθημα

	Χαμηλό		Μέτριο		Υψηλό	
	Σ	%	Σ	%	Σ	%
Η κυβερνοασφάλεια δεν μπορεί να προσφερθεί ως αυτόνομο μάθημα	55	55,0	37	37,0	8	8,0
Η Κυβερνοασφάλεια μπορεί να προσφερθεί ως αυτόνομο μάθημα	12	12,0	32	32,0	56	56,0
Η κυβερνοασφάλεια ΔΕΝ μπορεί να ενσωματωθεί στο αναλυτικό πρόγραμμα σπουδών	60	60,0	24	24,0	16	16,0
Η κυβερνοασφάλεια να ενσωματωθεί στο αναλυτικό πρόγραμμα σπουδών	10	10,0	20	20,0	70	70,0

Τέλος, οι συμμετέχοντες κλήθηκαν να δηλώσουν το ενδιαφέρον που θα είχαν οι μαθητές τους να μάθουν σχετικά με την κυβερνοασφάλεια κατά τη διάρκεια μιας σχολικής χρονιάς. Όπως παρουσιάζεται στον Πίνακα 6, οι περισσότεροι από τους συμμετέχοντες δήλωσαν ότι οι μαθητές θα είχαν υψηλό ενδιαφέρον να μάθουν για θέματα που

σχετίζονται με την κυβερνοασφάλεια (59%), την ιδιωτικότητα δεδομένων (63%), την κρυπτογράφηση (45%), τα δίκτυα και το διαδίκτυο (61%), την κωδικοποίηση και τον προγραμματισμό (51%), την κυβερνοτρομοκρατία (63%), την κυβερνοηθική (51%), τη ρομποτική (73%), το υλικό και λογισμικό των υπολογιστών (63%), τη συλλογή, αποθήκευση, χρήση και προστασία δεδομένων (57%), το hacking/ασφάλεια δεδομένων (63%), τον κυβερνονόμο (55%), την τεχνητή νοημοσύνη (59%) καθώς επίσης και τη μηχανική συστημάτων (54%).

Πίνακας 5: Ενδιαφέρον που θα είχαν οι μαθητές να μάθουν σχετικά με την κυβερνοασφάλεια κατά τη διάρκεια μιας σχολικής χρονιάς

	Χαμηλό		Μέτριο		Υψηλό	
	Σ	%	Σ	%	Σ	%
Βασικός ψηφιακός γραμματισμός	16	16,0	43	43,0	41	41,0
Θέματα που σχετίζονται με την κυβερνοασφάλεια	8	8,0	33	33,0	59	59,0
Ιδιωτικότητα δεδομένων	14	14,0	23	23,0	63	63,0
Κρυπτογράφηση	24	24,0	31	31,0	45	45,0
Δίκτυα και Διαδίκτυο	8	8,0	31	31,0	61	61,0
Οι μαθητές μου δεν ενδιαφέρονται για τίποτα	40	40,0	32	32,0	28	28,0
Κωδικοποίηση/Προγραμματισμός	12	12,0	37	37,0	51	51,0
Κυβερνοτρομοκρατία	10	10,0	27	27,0	63	63,0
Κυβερνοηθική	18	18,0	31	31,0	51	51,0
Ρομποτική	6	6,0	21	21,0	73	73,0
Υλικό και λογισμικό υπολογιστών	6	6,0	31	31,0	63	63,0
Συλλογή, αποθήκευση, χρήση και προστασία δεδομένων	12	12,0	31	31,0	57	57,0
Hacking/ ασφάλεια δεδομένων	10	10,0	27	27,0	63	63,0
Κυβερνονόμος	22	22,0	23	23,0	55	55,0
Τεχνητή νοημοσύνη	16	16,0	25	25,0	59	59,0
Μηχανική Συστημάτων	18	18,0	28	28,0	54	54,0

4.2.3 Προβλήματα και επιμέρους κατάρτιση

Το τελευταίο μέρος της παρούσας μελέτης είχε να κάνει με τα προβλήματα που θα μπορούσε να παρουσιαστούν κατά τη διδασκαλία του μαθήματος της κυβερνοασφάλειας στα σχολεία Μέσης Τεχνικής Εκπαίδευσης στην Κύπρο.

Οι συμμετέχοντες ερωτήθηκαν αν, κατά τη γνώμη τους, υπάρχουν προβλήματα τα οποία δεν αφήνουν τον τομέα της κυβερνοασφάλειας να μπορεί να διδαχθεί σε σχολική βάση. Σύμφωνα με τις απαντήσεις των συμμετεχόντων, οι μισοί (50%) δήλωσαν ότι υπάρχουν προβλήματα και οι άλλοι μισοί (50%) ότι δε υπάρχουν προβλήματα (Πίνακας 7).

Πίνακας 6: Προβλήματα

Κατά τη γνώμη σας υπάρχουν προβλήματα τα οποία δεν αφήνουν τον τομέα της κυβερνοασφάλειας να διδαχθεί σε σχολική βάση

	Συχνότητα	Ποσοστό %
Ναι	50	50.0
Όχι	50	50.0
Σύνολο	100	100.0

Από αυτούς που απάντησαν ότι θα υπάρχουν προβλήματα από την διδασκαλία του μαθήματος της κυβερνοασφάλειας στα σχολεία, οι περισσότεροι δήλωσαν ότι ο λόγος που απάντησαν Ναι ήταν ότι το μάθημα αυτό είναι κάτι εντελώς καινούργιο (26%). Επίσης, 8% δήλωσαν ότι είναι δύσκολο να διδαχθεί,6% ότι δεν θα βρεθεί ανταπόκριση από τους μαθητές, 4% ότι δεν μπορεί να στηριχθεί ένα τέτοιο μάθημα από εκπαιδευτές των Τεχνικών Σχολών της Κύπρου και ότι είναι Ανώτερου επιπέδου από το επίπεδο που διδάσκονται ήδη οι μαθητές και 2% ότι προκαλεί άγχος στους μαθητές (Πίνακας 8).

Πίνακας 7

Αν απαντήσατε Ναι στο προηγούμενο ερώτημα, επιλέξετε ποιο ή ποια από τα πιο κάτω αποτελεί πρόβλημα

	Συχνότητα	Ποσοστό %
Είναι κάτι εντελώς καινούργιο	26	26.0
Δεν μπορεί να υποστηριχθεί ένα τέτοιο μάθημα από εκπαιδευτές των Τεχνικών Σχολών στην Κύπρο	4	4.0
Είναι δύσκολο να διδαχθεί	8	8.0
Προκαλεί άγχος στους μαθητές	2	2.0
Είναι ανώτερου επιπέδου από το επίπεδο που διδάσκονται ήδη οι μαθητές	4	4.0
Δεν θα βρεθεί ανταπόκριση από τους μαθητές	6	6.0
Total	50	50.0
System	50	50.0
Total	100	100.0

Τέλος, οι εκπαιδευτικοί ερωτήθηκαν κατά πόσο θα ήθελαν να εκπαιδευτούν και να προετοιμαστούν να διδάξουν αυτό το μάθημα στους μαθητές τους. Οι περισσότεροι από τους συμμετέχοντες δήλωσαν ότι ήθελαν να το κάνουν αυτό με ποσοστό 92% (Πίνακας 9).

Πίνακας 8: Κατάρτιση

Θα θέλατε να εκπαιδευτείτε και να προετοιμαστείτε για να διδάξετε αυτό το μάθημα στους μαθητές σας;

	Συχνότητα	Ποσοστό %
Ναι	92	92.0
Όχι	8	8.0
Σύνολο	100	100.0

4.3 Συσχετίσεις

Για τον υπολογισμό των συσχετίσεων έχει χρησιμοποιηθεί το εργαλείο Independent Sample T-test για να φανεί κατά πόσο υπάρχει συσχέτιση μεταξύ των δύο φύλων και μεταξύ των δύο ειδικοτήτων όσον αφορά την ύπαρξη προβλημάτων στην εφαρμογή του μαθήματος της ασφάλειας στον Κυβερνοχώρο.

Η διαδικασία Independent-Samples T Test συγκρίνει τους μέσους για δύο ομάδες περιπτώσεων. Ιδανικά, για αυτό τον έλεγχο, τα άτομα θα πρέπει να χωριστούν τυχαία σε δύο ομάδες.

4.3.1 Σχέση φύλου και προβλημάτων στη διεξαγωγή του μαθήματος

Όπως φαίνεται και στους πίνακες που ακολουθούν δεν υπάρχει στατιστικά σημαντική διαφορά του φύλου ως προς το αν υπάρχουν προβλήματα στην διεξαγωγή του μαθήματος της κυβερνοασφάλειας στα σχολεία.

Tests of Normality

	Κατά τη γνώμη σας υπάρχουν προβλήματα τα οποία δεν αφήνουν τον τομέα της κυβερνοασφάλειας να διδαχθεί σε σχολική βάση	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Φύλο	Ναι	.411	50	.000	.608	50	.000
	Όχι	.431	50	.000	.588	50	.000

a. Lilliefors Significance Correction

Group Statistics

	Κατά τη γνώμη σας υπάρχουν προβλήματα τα οποία δεν αφήνουν τον τομέα της κυβερνοασφάλειας να διδαχθεί σε σχολική βάση	N	Mean	Std. Deviation	Std. Error Mean
Φύλο	Ναι	50	1.36	.485	.069
	Όχι	50	1.32	.471	.067

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Φύλο	Equal variances assumed	.694	.407	.418	98	.677	.040	.096	-.150	.230
	Equal variances not assumed			.418	97.920	.677	.040	.096	-.150	.230

4.3.2 Σχέση ειδικότητας και προβλημάτων στη διεξαγωγή του μαθήματος

Επιπλέον όσον αφορά την ειδικότητα και τα προβλήματα στη διεξαγωγή του μαθήματος, έχει φανεί ότι δεν υπάρχει στατιστικά σημαντική διαφορά ανάμεσα τους με p=.697>0.05.

Tests of Normality

	Κατά τη γνώμη σας υπάρχουν προβλήματα τα οποία δεν αφήνουν τον τομέα της κυβερνοασφάλειας να διδαχθεί σε σχολική βάση	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
		Statistic	df	Sig.	Statistic	df	Sig.
Ειδικότητα	Ναι	.370	50	.000	.632	50	.000
	Όχι	.360	50	.000	.634	50	.000

a. Lilliefors Significance Correction

Group Statistics

	Κατά τη γνώμη σας υπάρχουν προβλήματα τα οποία δεν αφήνουν τον τομέα της κυβερνοασφάλειας να διδαχθεί σε σχολική βάση	N	Mean	Std. Deviation	Std. Error Mean
Ειδικότητα	Ναι	50	1.56	.501	.071
	Όχι	50	1.46	.503	.071

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Ειδικότητα	Equal variances assumed	.153	.697	.995	98	.322	.100	.100	-.099	.299
	Equal variances not assumed			.995	97.998	.322	.100	.100	-.099	.299

4.3.3 Συσχετίσεις Pearson

Ο συντελεστής Pearson αποτελεί ένα συντελεστή γραμμικής συσχέτισης. Οι τιμές που λαμβάνει είναι από -1 μέχρι και 1, και συμβολίζεται με το r. Το Pearson χρησιμοποιείται κυρίως σε ποσοτικές μεταβλητές. Όταν λαμβάνει τιμές από -1 μέχρι -0.5 τότε θεωρείται ότι υπάρχει υψηλός αρνητικός συντελεστής της συσχέτισης, ενώ όταν λαμβάνει τιμές από 0.5 μέχρι 1 τότε θεωρείται ότι υπάρχει υψηλός θετικός συντελεστής συσχέτισης.

Οι υποθέσεις για τη συσχέτιση φύλου και του πόσο σημαντικού είναι να προσφέρεται το μάθημα ασφάλειας στον Κυβερνοχώρο είναι οι ακόλουθες:

H0: Δεν υπάρχει συσχέτιση μεταξύ των ειδικοτήτων και της γνώμης για το αν είναι σημαντικό να προσφέρεται το μάθημα στην Μέση Τεχνική Εκπαίδευση

H1: Υπάρχει συσχέτιση μεταξύ των ειδικοτήτων και της γνώμης για το αν είναι σημαντικό να προσφέρεται το μάθημα στην Μέση Τεχνική Εκπαίδευση

Μέσα από την ανάλυση έχει δημιουργηθεί ο Πίνακας Correlations. Κοιτάζοντας μόνο το κάτω τρίγωνο που σχηματίζει η διαγώνιος με τις μονάδες, ενδιαφέρει περισσότερο το Pearson Correlation, το οποίο είναι r=-0.194, γεγονός που παρουσιάζει χαμηλό αρνητικό συντελεστή συσχέτισης. Στη συνέχεια πρέπει να γίνει έλεγχος αν επαληθεύεται ή όχι το H0. Το p=0.053>0.05, συνεπώς δεν μπορεί να απορριφθεί η H0, και επομένως δεν υπάρχει συσχέτιση μεταξύ των ειδικοτήτων και της γνώμης για το αν είναι σημαντικό να προσφέρεται το μάθημα στην Μέση Τεχνική Εκπαίδευση.

Correlations

		Ειδικότητα	Κατά τη γνώμη σας, είναι σημαντικό να προσφέρεται το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική Εκπαίδευση;
Ειδικότητα	Pearson Correlation	1	-.194
	Sig. (2-tailed)		.053
	N	100	100
Κατά τη γνώμη σας, είναι σημαντικό να προσφέρεται το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική Εκπαίδευση;	Pearson Correlation	-.194	1
	Sig. (2-tailed)	.053	
	N	100	100

Οι υποθέσεις για τη συσχέτιση φύλου και του πόσο σημαντικού είναι να προσφέρεται το μάθημα ασφάλειας στον Κυβερνοχώρο είναι οι ακόλουθες:

H0: Δεν υπάρχει συσχέτιση μεταξύ των φύλων και της γνώμης για το αν είναι σημαντικό να προσφέρεται το μάθημα στην Μέση Τεχνική Εκπαίδευση

H1: Υπάρχει συσχέτιση μεταξύ των φύλων και της γνώμης για το αν είναι σημαντικό να προσφέρεται το μάθημα στην Μέση Τεχνική Εκπαίδευση

Μέσα από την ανάλυση έχει δημιουργηθεί ο Πίνακας Correlations. Κοιτάζοντας μόνο το κάτω τρίγωνο που σχηματίζει η διαγώνιος με τις μονάδες, ενδιαφέρει περισσότερο το Pearson Correlation, το οποίο είναι r=-0.233, γεγονός που παρουσιάζει χαμηλό αρνητικό συντελεστή συσχέτισης. Στη συνέχεια πρέπει να γίνει έλεγχος αν επαληθεύεται ή όχι το

Η0. Το p=0.020<0.05, συνεπώς απορρίπτεται η Η0 και επαληθεύεται η Η1, και επομένως υπάρχει συσχέτιση μεταξύ των φύλων και της γνώμης για το αν είναι σημαντικό να προσφέρεται το μάθημα στην Μέση Τεχνική Εκπαίδευση με τη σχέση να είναι στατιστικά σημαντική στο επίπεδο 0.05.

Correlations

		Φύλο	Κατά τη γνώμη σας, είναι σημαντικό να προσφέρεται το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική Εκπαίδευση;
Φύλο	Pearson Correlation	1	-.233*
	Sig. (2-tailed)		.020
	N	100	100
Κατά τη γνώμη σας, είναι σημαντικό να προσφέρεται το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική Εκπαίδευση;	Pearson Correlation	-.233*	1
	Sig. (2-tailed)	.020	
	N	100	100

*. Correlation is significant at the 0.05 level (2-tailed).

Κεφάλαιο 5 Συζήτηση

Η παρούσα διατριβή είχε σκοπό τη μελέτη των στάσεων και των απόψεων των εκπαιδευτικών Μηχανικής Ηλεκτρονικών Υπολογιστών και Ηλεκτρολογίας των Τεχνικών Σχολών της Κύπρου σχετικά με τη διδασκαλία της κυβερνοασφάλειας στα σχολεία.

Στην έρευνα αυτή έλαβαν μέρος 100 συνολικά εκπαιδευτικοί Μέσης Τεχνικής Εκπαίδευσης (66% άνδρες και 34% γυναίκες), ειδικοτήτων Μηχανικής Ηλεκτρονικών Υπολογιστών και Ηλεκτρολογίας. Οι περισσότεροι ήταν ηλικιών 36-45 ετών και ήταν εκπαιδευτές με Μεταπτυχιακό Τίτλο και εμπειρία 1-4 έτη.

Μέσα από τα αποτελέσματα της έρευνας αυτής έχει μελετηθεί η στάση και οι απόψεις των εκπαιδευτικών αναφορικά με τη διδασκαλία της κυβερνοασφάλειας στα σχολεία Μέσης Τεχνικής Εκπαίδευσης. Αναφορικά με τη στάση και τις απόψεις των εκπαιδευτικών, έχει φανεί ότι οι εκπαιδευτικοί δεν αφήνουν τους μαθητές τους να χρησιμοποιούν τα κινητά τους τηλέφωνα μέσα στην αίθουσα διδασκαλίας, είναι πρόθυμοι να μάθουν τους ιστότοπους που περιηγούνται οι μαθητές τους, έχουν επίγνωση και ενδιαφέρονται για την ασφάλεια των μαθητών τους, γνωρίζουν τις εφαρμογές κοινωνικής δικτύωσης με τις οποίες αλληλεπιδρούν οι μαθητές τους, στηρίζουν ότι τα μέτρα ασφαλείας για τους μαθητές τους είναι απαραίτητα, είναι πρόθυμοι να διδαχθούν για την ασφάλεια στον κυβερνοχώρο, γνωρίζουν τα εγκλήματα στον κυβερνοχώρο στα οποία ενδέχεται να εκτεθούν οι μαθητές τους, γνωρίζουν σχετικά με τον νόμο περί εγκλημάτων στον τομέα της πληροφορικής, συμφωνούν απόλυτα στο γεγονός ότι οι μαθητές των σχολείων πρέπει να διδάσκονται διεξοδικά για την ασφάλεια στον κυβερνοχώρο, εξετάζουν το ιστορικό των μαθητών τους στο πρόγραμμα περιήγησης στο διαδίκτυο, συμφωνούν να χρησιμοποιήσουν οποιονδήποτε τύπο προγράμματος που παρακολουθεί την πρόσβαση των μαθητών σε συγκεκριμένους ιστότοπους, γνωρίζουν την πολιτική ασφαλούς χρήσης του διαδικτύου στο σχολείο τους και γνωρίζουν σε ποιον να αναφέρονται εάν αντιμετωπίζουν προβλήματα ασφάλειας στον κυβερνοχώρο στο σχολείο τους. Επίσης, οι περισσότεροι από τους συμμετέχοντες συμφωνούν με τη στάση ότι παρατηρούν την αλληλεπίδραση των μαθητών τους με συγκεκριμένους ιστότοπους στο διαδίκτυο, γνωρίζουν για τα δικαιώματα του παιδιού όσον αφορά το νόμο για τη διαδικτυακή δραστηριότητα, επιτρέπουν στους μαθητές τους

να χρησιμοποιούν το διαδίκτυο με όλα τα διαθέσιμα μέσα (κινητό smartphone ή οποιοδήποτε τύπο έξυπνης συσκευής). Επίσης, έχει φανεί, οι περισσότεροι από τους συμμετέχοντες διαφωνούν απόλυτα με τη στάση ότι οι μαθητές τους δεν θα απειληθούν ποτέ λόγω της χρήσης του Διαδικτύου.

Γενικά, έχει φανεί ότι οι εκπαιδευτικοί έχουν μια θετική στάση απέναντι στη διδασκαλία του μαθήματος της κυβερνοασφάλειας. Κρατούν δηλαδή μια ενθαρρυντική στάση. Όμοια, τα αποτελέσματα μιας άλλης έρευνας έχουν δείξει ότι οι συνεργατικές σκηνές με ενθαρρυντικούς και υποστηρικτικούς εκπαιδευτές συμβάλλουν στο αυξημένο ενδιαφέρον των παιδιών στον τομέα της κυβερνοασφάλειας [33].

Μέσα από αυτή τους την στάση η εκπαιδευτικοί δηλώνουν ότι είναι ευαισθητοποιημένοι με το θέμα της ασφάλειας στον κυβερνοχώρο. Όμοια, μια άλλη έρευνα, [31], δηλώνει ότι η κοινότητα ασφαλείας μπορεί να εγγράψει και να παρασύρει τους εφήβους στην ασφάλεια στον κυβερνοχώρο και να αυξήσει τον βαθμό ευαισθητοποίησης σχετικά με την ασφάλεια.

Αντίθετα, σε μια έρευνα, έχει φανεί ότι οι συμμετέχοντες δεν είχαν την απαιτούμενη γνώση και κατανόηση της σημασίας των αρχών ασφάλειας πληροφοριών και της πρακτικής εφαρμογής τους στην καθημερινή τους εργασία [30].

Ακόμα, έχει φανεί ότι οι περισσότεροι συμμετέχοντες θεωρούν πολύ σημαντικό να προσφέρεται το μάθημα της κυβερνοασφάλειας στη Μέση Τεχνική Εκπαίδευση. Το ίδιο συμφωνούν και σε άλλες έρευνες καθώς προτείνεται ευθυγράμμιση του διδακτικού περιεχομένου με τα ενδιαφέροντα των μαθητών [32].

Επιπλέον, οι εκπαιδευτικοί, προτείνουν την ενσωμάτωση του μαθήματος της κυβερνοασφάλειας στο Αναλυτικό Πρόγραμμα, την προσφορά του ως αυτόνομο μάθημα, ως διαγωνισμό και λιγότερο ως εξωσχολική δραστηριότητα.

Επιπλέον, μέσα από τα αποτελέσματα της έρευνας αυτής, έχει φανεί ότι οι εκπαιδευτικοί αξιολόγησαν το επίπεδο ενδιαφέροντος των μαθητών ως υψηλό όσον αφορά τις σχολικές δραστηριότητες και Διαγωνισμούς και μέτριο όσον αφορά τα Εξωσχολικά/Σωματεία.

Επιπρόσθετα, οι εκπαιδευτικοί ήταν θετικοί όταν κλήθηκαν να δηλώσουν κατά πόσο θα υπήρχε ενδιαφέρον από τους μαθητές ώστε το μάθημα της κυβερνοασφάλειας να προσφέρεται ως αυτόνομο μάθημα και κατά πόσο θα μπορούσε να ενσωματωθεί στο Αναλυτικό Πρόγραμμα Σπουδών. Όπως έχει φανεί οι εκπαιδευτικοί δήλωσαν, με υψηλό ενδιαφέρον, ότι η κυβερνοασφάλεια μπορεί να προσφερθεί ως αυτόνομο μάθημα και ότι η κυβερνοασφάλεια μπορεί να ενσωματωθεί στο Αναλυτικό Πρόγραμμα Σπουδών.

Ακόμα, οι εκπαιδευτικοί δήλωσαν ότι μαθητές θα είχαν υψηλό ενδιαφέρον να μάθουν για θέματα που σχετίζονται με την κυβερνοασφάλεια, την ιδιωτικότητα δεδομένων, την κρυπτογράφηση, τα δίκτυα και το διαδίκτυο, την κωδικοποίηση και τον προγραμματισμό, την κυβερνοτρομοκρατία, την κυβερνοηθική, τη ρομποτική, το υλικό και λογισμικό των υπολογιστών, τη συλλογή, αποθήκευση, χρήση και προστασία δεδομένων, το hacking/ασφάλεια δεδομένων, τον κυβερνονόμο, την τεχνητή νοημοσύνη καθώς επίσης και τη μηχανική συστημάτων.

Επίσης, όσον αφορά τα προβλήματα που θα μπορούσε να παρουσιαστούν κατά τη διδασκαλία του μαθήματος της κυβερνοασφάλειας στα σχολεία Μέσης Τεχνικής Εκπαίδευσης στην Κύπρο οι μισοί από τους συμμετέχοντες δήλωσαν ότι θα υπάρχουν προβλήματα και οι άλλοι μισοί ότι δε θα υπάρχουν προβλήματα. Από αυτούς που απάντησαν ότι θα υπάρχουν προβλήματα από την διδασκαλία του μαθήματος της κυβερνοασφάλειας στα σχολεία, οι περισσότεροι δήλωσαν ότι ο λόγος που απάντησαν Ναι ήταν ότι το μάθημα αυτό είναι κάτι εντελώς καινούργιο.

Τέλος, οι εκπαιδευτικοί εξέφρασαν το ενδιαφέρον τους για να εκπαιδευτούν και να προετοιμαστούν να διδάξουν αυτό το μάθημα της κυβερνοασφάλειας στους μαθητές τους. Το ίδιο επισημαίνεται και σε άλλες έρευνες καθώς πρέπει να παρέχεται εκπαίδευση για τη βέλτιστη πρακτική στο διαδίκτυο [2].

Κεφάλαιο 6 Συμπεράσματα-Προτάσεις-Εισηγήσεις

Η έλλειψη δεξιοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο λαμβάνει διαδεδομένες διαστάσεις. Ένας τρόπος για να διασφαλιστεί ένα μεγαλύτερο κύκλωμα στον τομέα της κυβερνοασφάλειας είναι να εκπαιδευτούν περισσότεροι καθηγητές γυμνασίου ώστε όχι μόνο να διδάσκουν την κυβερνοασφάλεια στα σχολεία τους ή να ενσωματώνουν έννοιες κυβερνοασφάλειας στις τάξεις τους, αλλά και να προάγουν την ασφάλεια πληροφορικής ως ελκυστικό επαγγελματικό μονοπάτι. Η προτεινόμενη έρευνα θα οδηγήσει στην ανάπτυξη ενός μοναδικού και καινοτόμου προγράμματος σπουδών και κλιμακούμενου προγράμματος στον τομέα της κυβερνοασφάλειας και ενός συνόλου ισχυρών εργαλείων για μια διασκεδαστική μαθησιακή εμπειρία στην εκπαίδευση στον κυβερνοχώρο.

Το θέμα της κυβερνοασφάλειας αφορά τους ανθρώπους, θεωρώντας ότι όλοι χρησιμοποιούν ψηφιακές τεχνολογίες τόσο στην επαγγελματική όσο και στην ιδιωτική ζωή και ότι η συμπεριφορά των ανθρώπων παίζει σημαντικό ρόλο στην εμφάνιση κυβερνοαπειλών. Ο ανθρώπινος παράγοντας πρέπει επομένως να αναγνωριστεί ως βασικό στοιχείο που πρέπει να ληφθεί υπόψη για την ανάπτυξη μιας αποτελεσματικής ασφάλειας στον κυβερνοχώρο και η εκπαίδευση είναι ο βασικός μοχλός. Ωστόσο, δεδομένου ότι τα παιδιά έχουν πρόσβαση σε διαδικτυακές δραστηριότητες από νεαρή ηλικία, είναι συνετό να αναπτυχθούν παρεμβάσεις για την προώθηση της ψηφιακής ευαισθητοποίησης από τα πρώτα χρόνια στο σχολείο, εστιάζοντας στην υπεύθυνη χρήση των ψηφιακών τεχνολογιών. Το να συνειδητοποιήσουν τους κινδύνους στους οποίους εκτίθενται είναι ένα σημαντικό βήμα για να κινούνται με ασφάλεια τα παιδιά στο Διαδίκτυο και να κατανοούν τους διάφορους κινδύνους στον κυβερνοχώρο που πρέπει να αντιμετωπίσουν.

Πράγματι, οι μαθητές θα πρέπει να είναι προετοιμασμένοι να αναγνωρίζουν τους κινδύνους όταν χρησιμοποιούν ψηφιακές τεχνολογίες: όχι μόνο τον διαδικτυακό εκφοβισμό, θα πρέπει να δίνουν μεγαλύτερη προσοχή στην προστασία των προσωπικών

τους δεδομένων και στην αξιοπιστία των ειδήσεων στα μέσα κοινωνικής δικτύωσης. Όλοι οι χρήστες του κυβερνοχώρου πρέπει να εκπαιδεύονται για τη σημασία των βέλτιστων πρακτικών στο Διαδίκτυο. Επιπλέον, οι μαθητές στο επίπεδο της Μέσης Τεχνικής εκπαίδευσης είναι μεγάλοι χρήστες του Διαδικτύου και θα αποτελούν το μελλοντικό εργατικό δυναμικό. Τέτοιοι παράγοντες απαιτούν την εκπαίδευση των μαθητών σχετικά με περιστατικά ασφάλειας στον κυβερνοχώρο. Αν και τα αυξανόμενα περιστατικά ασφάλειας στον κυβερνοχώρο ενδέχεται να μην εξαλειφθούν πλήρως με εκπαίδευση και κατάρτιση, οι χρήστες του Διαδικτύου πρέπει να εκπαιδεύονται ώστε να αυξάνουν την ευαισθητοποίησή τους για αυτά τα συμβάντα, ώστε να μπορούν να λαμβάνουν προληπτικά μέτρα όταν είναι απαραίτητο. Οι μαθητές πρέπει να έχουν τη δυνατότητα να προστατεύουν τον εαυτό τους. Η αυτοάμυνα είναι η καλύτερη ασπίδα όταν γίνεται χρήση του Διαδικτύου.

Επιπλέον, η εκπαίδευση στην τεχνολογία των πληροφοριών είναι απαραίτητη, καθώς η ζωή της επόμενης γενιάς μας θα εξαρτηθεί από αυτήν χωρίς αμφιβολία. Επιπλέον, το εκπαιδευτικό ίδρυμα εμπλέκεται σε αυτό το θέμα όπου τα σχολεία μέσης εκπαίδευσης προσφέρουν στους μαθητές βασικά μαθήματα τεχνολογίας πληροφοριών που είναι καλό αλλά, δυστυχώς, συνήθως αγνοούν τα μαθήματα ασφάλειας. Αυτό είναι ένα κρίσιμο σφάλμα που οδηγεί σε έλλειψη ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο για τους ανθρώπους. Οι μαθητές μαθαίνουν πώς να είναι ασφαλείς και γιατί μπορούν να έχουν θετικό κρίσιμο αντίκτυπο στην κοινωνία. Έτσι, τα σχολεία Μέσης Εκπαίδευσης θα πρέπει να διαθέτουν ένα πρόγραμμα ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο.

Η ασφάλεια στον κυβερνοχώρο πρέπει να είναι μέλημα όλων. Όλο και περισσότερα περιστατικά ασφάλειας στον κυβερνοχώρο αναφέρονται καθώς περισσότεροι χρήστες έχουν πρόσβαση στο διαδίκτυο. Ωστόσο, το να γνωρίζεις και να χρησιμοποιείς καλές πρακτικές δεν σημαίνει ότι είσαι εκατό τοις εκατό προστατευμένος. Στην ακαδημία, τόσο οι μαθητές όσο και οι εκπαιδευτικοί πρέπει να εκπαιδεύονται όσον αφορά την ευαισθητοποίηση σχετικά με την ασφάλεια και τις καλές πρακτικές. Ως εκπαιδευτικοί, η ευθύνη της εκπαίδευσης των νέων σχετικά με την ασφάλεια στον κυβερνοχώρο βαρύνει κυρίως τους εκπαιδευτικούς.

Η έρευνα αυτή καλείτο να απαντήσει σε 4 ερευνητικά ερωτήματα.

Το πρώτο και δεύτερο ερευνητικό ερώτημα αφορούσε τη στάση και τις απόψεις των εκπαιδευτικών ως προς τη διδασκαλία της κυβερνοασφάλειας στα σχολεία.

Το τρίτο ερευνητικό ερώτημα αφορούσε τους τρόπους με τους οποίους μπορεί να προσφερθεί το μάθημα στην Μέση Τεχνική Εκπαίδευση, και το τέταρτο ερευνητικό ερώτημα είχε να κάνει με το πώς το μάθημα μπορεί να προσαρμοστεί στις ανάγκες του κάθε εκπαιδευόμενου.

Όπως έχει φανεί μέσα από τα αποτελέσματα της παρούσας μελέτης, έχουν απαντηθεί όλα τα ερευνητικά ερωτήματα που έχουν τεθεί στην αρχή της παρούσας μελέτης. Κατ' αρχάς έχουν φανεί οι προθέσεις των εκπαιδευτικών να αναλάβουν να διδάξουν το μάθημα της ασφάλειας στον κυβερνοχώρο στη Μέση Τεχνική Εκπαίδευση οι οποίες φαίνεται να είναι αρκετά ενθαρρυντικές. Επιπλέον, έχουν προταθεί τρόποι για την διδασκαλία του μαθήματος αυτού καθώς επίσης και τρόποι σύμφωνα με τους οποίους μπορεί να προσαρμοστεί στις ανάγκες των εκπαιδευόμενων, όπως είναι για παράδειγμα η ενσωμάτωσή του στο Αναλυτικό Πρόγραμμα ή η διδασκαλία του ως αυτόνομο μάθημα ή ακόμα και η συμμετοχή των παιδιών σε διαγωνισμούς.

Στην έρευνα αυτή, όπως και σε κάθε έρευνα, υπήρχαν κάποιοι περιορισμοί. Κατ' αρχάς, ο χρόνος ήταν αρκετά λίγος για να μπορεί να ολοκληρωθεί. Επίσης, οι συμμετέχοντες έπρεπε να προέρχονται μόνο από δύο ειδικότητες. Συνεπώς αυτό στένευε κατά κάποιο τρόπο τα περιθώρια ολοκλήρωσής της. Ακόμα, λόγω του φόρτου εργασία τους, οι εκπαιδευτικοί άργησαν να συμπληρώσουν το ηλεκτρονικό ερωτηματολόγιο, γεγονός που οδηγούσε σε καθυστέρηση στην ολοκλήρωση της Ανάλυσης των δεδομένων.

Εν κατακλείδι, είναι σημαντικό να γίνει μια όμοια έρευνα σε παγκύπριο επίπεδο που να αφορά όλες τις βαθμίδες της εκπαίδευσης έτσι ώστε να εξαχθούν ακόμα πιο αξιόπιστα αποτελέσματα.

Παράρτημα
Ερωτηματολόγιο

Ερωτηματολόγιο Έρευνας με Τίτλο:

Η Διδασκαλία της Κυβερνοασφάλειας στη Μέση Τεχνική Εκπαίδευση

Αγαπητοί Συμμετέχοντες,
Σας προσκαλώ να συμμετάσχετε σε μια ερευνητική εργασία με τίτλο: Η Διδασκαλία της Κυβερνοασφάλειας στη Μέση Τεχνική Εκπαίδευση. Αυτήν τη στιγμή είμαι εγγεγραμμένη στο Μεταπτυχιακό Πρόγραμμα Ασφάλεια Υπολογιστών και Δικτύων του Ανοικτού Πανεπιστημίου Κύπρου και είμαι στη διαδικασία συγγραφής της μεταπτυχιακής μου διατριβής. Σκοπός της έρευνας είναι η διεξοδική μελέτη των στάσεων και των απόψεων των εκπαιδευτικών πληροφορικής και ηλεκτρολογία των Τεχνικών Σχολών της Κύπρου σχετικά με τη διδασκαλία της κυβερνοασφάλειας στα σχολεία. Το ερωτηματολόγιο που επισυνάπτεται έχει σχεδιαστεί για να συλλέγει πληροφορίες σχετικά με: τις στάσεις και απόψεις των εκπαιδευτικών ως προς την διδασκαλία της κυβερνοασφάλειας στα σχολεία, τους τρόπους μέσα από τους οποίους μπορεί να προσφερθεί το μάθημα αυτό στην Μέση Εκπαίδευση καθώς και το πώς μπορεί το μάθημα αυτό να προσαρμοστεί στις ανάγκες του κάθε εκπαιδευόμενου.
Η συμμετοχή σας σε αυτό το ερευνητικό έργο είναι απολύτως εθελοντική. Μπορείτε να αρνηθείτε εντελώς ή να αφήσετε κενές οποιεσδήποτε ερωτήσεις δεν θέλετε να απαντήσετε. Οι απαντήσεις σας θα παραμείνουν εμπιστευτικές και ανώνυμες. Τα δεδομένα από αυτήν την έρευνα θα διατηρούνται υπό κλείδωμα και θα αναφέρονται μόνο ως συλλογικό συνδυασμένο σύνολο. Κανείς άλλος εκτός από την ερευνήτρια δεν θα γνωρίζει τις ατομικές σας απαντήσεις σε αυτό το ερωτηματολόγιο.
Εάν συμφωνείτε να συμμετάσχετε σε αυτό το έργο, απαντήστε στις ερωτήσεις του ερωτηματολογίου με συνέπεια και αληθοφάνεια. Θα χρειαστούν περίπου 10-12 λεπτά για να ολοκληρωθεί.
Εάν έχετε οποιεσδήποτε ερωτήσεις σχετικά με αυτό το έργο, μη διστάσετε να επικοινωνήσετε μαζί μου στο andry.christofi@st.ouc.ac.cy.

Σας ευχαριστώ για τη βοήθειά σας σε αυτή τη σημαντική προσπάθεια.

Μετά τιμής,
Άντρη Χριστοφή

ΜΕΡΟΣ Ι: ΔΗΜΟΓΡΑΦΙΚΑ ΣΤΟΙΧΕΙΑ

1. Φύλο
    - ☐ Άνδρας
    - ☐ Γυναίκα

2. Ηλικία
    - ☐ 25-35 ετών
    - ☐ 36-45 ετών
    - ☐ 46-55 ετών
    - ☐ 56-65 ετών

3. Οργανική Θέση
    - ☐ Εκπαιδευτής
    - ☐ Βοηθός Διευθυντής
    - ☐ Διευθυντής

4. Ειδικότητα
    - ☐ Ηλεκτρολογία
    - ☐ Μηχανικής Ηλεκτρονικών Υπολογιστών

5. Εκπαίδευση
    - ☐ Πτυχίο
    - ☐ Μεταπτυχιακό
    - ☐ Διδακτορικό

6. Εμπειρία
    - ☐ 1-4 χρόνια
    - ☐ 5-10 χρόνια
    - ☐ > 10 χρόνια

ΜΕΡΟΣ ΙΙ: ΚΥΡΙΩΣ ΕΡΕΥΝΑ

Η στάση και οι απόψεις των εκπαιδευτικών ως προς την διδασκαλία της κυβερνοασφάλειας στα σχολεία

1. Γνώση της σημασίας της κυβερνοασφάλειας για τους μαθητές. Παρακαλώ όπως επισημάνετε το βαθμό που συμφωνείτε με τις ακόλουθες εκφράσεις (1- Συμφωνώ απόλυτα, 2- Συμφωνώ, 3- Ούτε συμφωνώ ούτε διαφωνώ, 4- Διαφωνώ, 5-Διαφωνώ απόλυτα).

Α/Α	Έκφραση	1	2	3	4	5
1	Δεν αφήνω τους μαθητές μου να χρησιμοποιούν τα κινητά τους τηλέφωνα μέσα στην αίθουσα διδασκαλίας					
2	Παρατηρώ την αλληλεπίδραση των μαθητών μου με συγκεκριμένους ιστότοπους στο Διαδίκτυο					
3	Είμαι πρόθυμος να μάθω τους ιστότοπους που περιηγούνται οι μαθητές μου					
4	Έχω επίγνωση και ενδιαφέρομαι για την ασφάλεια των μαθητών μου					
5	Γνωρίζω τις εφαρμογές κοινωνικής δικτύωσης με τις οποίες αλληλεπιδρούν οι μαθητές μου					
6	Νομίζω ότι τα μέτρα ασφαλείας για τους μαθητές μου είναι απαραίτητα					
7	Νομίζω ότι οι μαθητές μου δεν θα απειληθούν ποτέ λόγω της χρήσης του Διαδικτύου					
8	Γνωρίζω για τα δικαιώματα του παιδιού όσον αφορά το νόμο για τη διαδικτυακή δραστηριότητα					
9	Έχω λάβει εκπαίδευση για την ασφάλεια στον κυβερνοχώρο για τους μαθητές μου					
10	Είμαι πρόθυμος να διδαχθώ για την ασφάλεια στον κυβερνοχώρο					
11	Γνωρίζω τα εγκλήματα στον κυβερνοχώρο στα οποία ενδέχεται να εκτεθούν οι μαθητές μου					
12	Γνωρίζω σχετικά με τον νόμο περί εγκλημάτων στον τομέα της πληροφορικής					
13	Οι μαθητές των σχολείων πρέπει να διδάσκονται διεξοδικά για την ασφάλεια στον κυβερνοχώρο					
14	Επιτρέπω στους μαθητές μου να χρησιμοποιούν το διαδίκτυο με όλα τα διαθέσιμα μέσα (κινητό smartphone ή οποιοδήποτε τύπο έξυπνης συσκευής)					
15	Εξετάζω το ιστορικό των μαθητών μου στο πρόγραμμα περιήγησης στο Διαδίκτυο					

16	Συμφωνώ να χρησιμοποιήσω οποιονδήποτε τύπο προγράμματος που παρακολουθεί ή περιορίζει την πρόσβαση των μαθητών σε συγκεκριμένους ιστότοπους ή λήψεις εφαρμογών					
17	Γνωρίζω την πολιτική ασφαλούς χρήσης του Διαδικτύου στο σχολείο μου					
18	Γνωρίζω σε ποιον αναφέρω εάν αντιμετωπίζω προβλήματα ασφάλειας στον κυβερνοχώρο στο σχολείο μου.					

Τρόποι που μπορεί να προσφερθεί το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική Εκπαίδευση

1. Κατά τη γνώμη σας, είναι σημαντικό να προσφέρεται το μάθημα της κυβερνοασφάλειας στην Μέση Τεχνική Εκπαίδευση;
   - ☐ Πολύ σημαντικό
   - ☐ Σημαντικό
   - ☐ Λίγο σημαντικό
   - ☐ Καθόλου σημαντικό

2. Πώς, κατά τη γνώμη σας, η δημόσια εκπαίδευση μπορεί να παρέχει εκπαίδευση για την ασφάλεια στον κυβερνοχώρο για τους μαθητές των τεχνικών σχολών;
   - ☐ Έχει ενσωματωθεί στο αναλυτικό πρόγραμμα
   - ☐ Ως μέρος εξωσχολικού ή συλλόγου
   - ☐ Ως αυτόνομο μάθημα
   - ☐ Ως διαγωνισμός
   - ☐ Ως σχολική δραστηριότητα

3. Πώς θα αξιολογούσατε το επίπεδο ενδιαφέροντος των μαθητών σας να μάθουν περισσότερα για την ασφάλεια στον κυβερνοχώρο σε: (1-Χαμηλή, 2-Μέτρια, 3-Υψηλή)

A/A	Έκφραση	1	2	3
1	Εξωσχολικά / Σωματεία			
2	Σχολικές Δραστηριότητες			
3	Διαγωνισμοί			

4. Κατά πόσο οι μαθητές σας ενδιαφέρονται να μάθουν περισσότερα για την κυβερνοασφάλεια. (1-χαμηλό ενδιαφέρον, 2-μέτριο ενδιαφέρον, 3-υψηλό ενδιαφέρον)

A/A	Έκφραση	1	2	3
1	Η κυβερνοασφάλεια δεν μπορεί να προσφερθεί ως αυτόνομο μάθημα			
2	Κυβερνοασφάλεια μπορεί να προσφερθεί ως αυτόνομο μάθημα			
3	Η κυβερνοασφάλεια ΔΕΝ μπορεί να ενσωματωθεί στο αναλυτικό πρόγραμμα σπουδών			
4	Η κυβερνοασφάλεια να εισαχθεί στο αναλυτικό πρόγραμμα σπουδών			

5. Τι από τα πιο κάτω θα μπορούσαν να μάθουν οι μαθητές σας κατά την διάρκεια μιας σχολικής χρονιάς; (1-χαμηλό ενδιαφέρον, 2-μέτριο ενδιαφέρον, 3-υψηλό ενδιαφέρον)

A/A	Έκφραση	1	2	3
1	Βασικός ψηφιακός γραμματισμός			
2	θέματα που σχετίζονται με την κυβερνοασφάλεια φέτος στην τάξη			
3	Ιδιωτικότητα δεδομένων			
4	Κρυπτογράφηση			
5	Δίκτυα και Διαδίκτυο			
6	Οι μαθητές μου δεν έχουν μάθει για κανένα			
7	Κωδικοποίηση/Προγραμματισμός			
8	Κυβερνοτρομοκρατία/Κυβερνοτρομοκρατία			
9	Κυβερνοηθική			
10	Ρομποτική			
11	Υλικό και λογισμικό υπολογιστών			

12	Συλλογή, αποθήκευση, χρήση και προστασία δεδομένων			
13	Hacking/ασφάλεια δεδομένων			
14	Κυβερνονόμος			
15	Τεχνητή νοημοσύνη			
16	Μηχανική Συστημάτων			

Προβλήματα

1. Κατά τη γνώμη σας, υπάρχουν προβλήματα τα οποία δεν αφήνουν τον τομέα της κυβερνοασφάλειας να μπορεί να διδαχθεί σε σχολική βάση;

   ☐ Ναι

   ☐ Όχι

2. Αν απαντήσατε Ναι στο προηγούμενο ερώτημα, τότε επιλέξετε ποιο ή ποια από τα πιο κάτω αποτελεί πρόβλημα για τη διεξαγωγή αυτού του μαθήματος στα σχολεία Μέσης Τεχνικής Εκπαίδευσης στην Κύπρο:

   ☐ Είναι κάτι εντελώς καινούργιο

   ☐ Δεν μπορεί να υποστηριχθεί ένα τέτοιο μάθημα από εκπαιδευτές των Τεχνικών Σχολών στην Κύπρο

   ☐ Είναι δύσκολο να διδαχθεί

   ☐ Δεν αποτελεί ενδιαφέρον μάθημα

   ☐ Προκαλεί άγχος στους μαθητές

   ☐ Είναι ανώτερου επιπέδου από το επίπεδο που διδάσκονται ήδη οι μαθητές

   ☐ Δεν θα βρεθεί ανταπόκριση από τους μαθητές

   ☐ Άλλο…….

3. Θα θέλατε να εκπαιδευτείτε και να προετοιμαστείτε για να διδάξετε αυτό το μάθημα στους μαθητές σας;

   ☐ Ναι

   ☐ Όχι

Βιβλιογραφία

[1] I. Venter , R. Blignaut, K. Renaud και A. Venter, «"Cyber security education is an essential as "the three R's",» *Hellyon,* τόμ. 5, αρ. 12, p. e02855, 2019.

[2] L. Muniandy, B. Muniandy και Z. Samsudin, «Cyber Security Behavior among Higher Education Students in Malaysia,» *Journal of Information Assurance & Cybersecurity,* αρ. 1-13, 2017.

[3] A. Lodgher, J. Yang και U. Bulut, «An innovative Modular Approach of Teaching Cyber Security across Computing Curricula,» σε *IEEE Frontiers in Education Conference (FIE)*, CA, USA, 2018.

[4] R. Anderson και G. Romney, «Student experiential learning of cyber security through virtualization,» *Journal of Research in Innovative Teaching,* τόμ. 7, αρ. 1, 2014.

[5] M. Richardson, P. Lemoine, W. Stephens και W. Waller, «Planning for Cyber Security in Schools: The Human Factor,» *ERIC,* τόμ. 27, αρ. 2, pp. 23-39, 2020.

[6] C. Kruse, «Cybersecurity in healthcare: A systematic review of modern threats and trends,» *Technology and Health Care,* τόμ. 25, αρ. 1, pp. 1-10, 2017.

[7] P. Dong, «A systematic review of studies on cyber physical system security,» *International Journal of Security and Its Applications,* τόμ. 9, αρ. 1, pp. 155-164, 2015.

[8] A. Herrera, M. Ron και C. Rabadão, «National cyber-security policies oriented to BYOD (bring your own device): Systematic review,» σε *12th Iberian Conference on Information Systems and Technologies (CISTI)*, 2017.

[9] N. Ahmad, U. Mokhtar και Z. Hood, «Cyber security situational awareness among parents,» σε *Cyber Resilience Conference*, Putrajaya Malaysia, 2019.

[10] R. Hamid, Z. Yunos και M. Ahmad, «Cyber parenting module development for parents,» σε *Proc. INTED2018 Conference*, Valencia, Spain, March 2018.

[11] B. Horowitz και D. Scott Lucero, «System-Aware Cyber Security: A Systems Engineering Approach for Enhancing Cyber Security,» *Insight ,* τόμ. 19, pp. 39-42, 2016.

[12] M. Rademaker, «Assessing Cyber Security 2015,» *Information & Security:An International Journal,* τόμ. 34, pp. 93-104, 2016.

[13] S. Hart, M. Andrea, P. Federica και S. Vladimiro, «Risk: A Serious Game for Cyber Security Awareness And Education,» *Computers & Security,* τόμ. 95, 2020.

[14] W. Trappe και J. Straub, «Journal of Cybersecurity and Privacy: A New Open Access Journal,» *Journal of Cybersecurity and Privacy,* τόμ. 1, pp. 1-3, 2021.

[15] L. Fichtner, «What Kind of Cyber Security? Theorising Cyber Security and Mapping Approaches,» *Internet Policy Review,* τόμ. 7, pp. 1-19, 2018.

[16] S. Pawar, R. Mente και B. Chendage, «Cyber Crime, Cyber Space and Effects of Cyber Crime,» *International Journal of Scientific Research in Computer Science,Engineering and Information Technology,* τόμ. 7, pp. 210-214, 2021.

[17] M. Keith, «Cyber Security Education, Qualifications and Training,» *Holloway, R., Ed., Engineering & Technology Reference, Institution of Engineering and Technology,* pp. 1-11, 2015.

[18] H. H. Park, «A Study on Cyber Crime Deterrence Recognition: The Influence of Recognition of Punishment for Cyber Crime on Intention to Report Crime,» *Korean Criminal Psychology Research,* τόμ. 16, pp. 85-98, 2020.

[19] P. Seemma, S. Nandhini και M. Sowmiya, «Overview of Cyber Security,» *IJARCCE,* τόμ. 7, pp. 125-128, 2018.

[20] N. Diakun-Thibault, «Defining Cybersecurity,» *Technology Innovation Management Review,* 2014.

[21] M. Natalia, «INTERNET IN EDUCATION-INTERNET SAFETY ISSUES AND ELEMENTS OF EDUCATION IN THIS AREA,» *NATIONAL PEDAGOGICAL DRAHOMANOV UNIVERSITY,* p. 123, 2022.

[22] L. De Kimpe, M. Walrave, K. Ponnet και J. Van Ouyts, «Internet safety,» *The international encyclopedia of media literacy,* pp. 1-11, 2019.

[23] K. Olson, M. O'Brien, W. Rogers και N. Charness, «Diffusion of technology: Frequency of use for younger and older adults,» *Ageing International,* τόμ. 36, αρ. 1, pp. 123-145, 2011.

[24] S. Livingstone, L. Haddon, A. Gorzing και K. Olafsson, «Risks and safety onhe Internet: The perspective of European children,» *Full Findings,* 2011.

[25] Youth Protection Roundtable, «Youth protection roundtable toolkit. EC Safer Internet Programme,» 2009.

[26] B. Velicu και M. Barbovschi, «Internet access, uses, risks and opportunities for children in Romania,» *EU Kids Online 2018 results, EU Kids Online and DigiLiv-REI,* 2019.

[27] S. Molter, G. Martinez, G. Garmendia, J. Croll και A. Järventaus, «Children's rights in the digital space, Observatory for sociopolitical developments in Europe,» 2021.

[28] Europol, «Internet Organised Crime Threat Assessment (IOCTA) 2021,» *Publications Office of the European Union, Luxembourg,* 2021.

[29] G. Jin, M. Tu, T. Kim, J. Heffron και J. White, «Game based cybersecurity training for high school students,» σε *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 2018.

[30] M. Olano, L. Oliva, R. Cox, D. Firestone, O. Kubik και D. Thomas, «{SecurityEmpire}: Development and Evaluation of a Digital Game to Promote Cybersecurity Education,» σε *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[31] A. Lédeczi, M. MarÓti, H. Zare, B. Yett, N. Hutchins, B. Broll και G. Biswas, «Teaching cybersecurity with networked robots,» σε *50th ACM Technical Symposium on Computer Science Education*, 2019.

[32] K. Jones, A. Namin και M. Armstrong, «What Should Cybersecurity Students Learn in School? Results from Interviews with Cyber Professionals,» σε *IProceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science*, 2017.

[33] I. Chen και L. Shen, «The cyberethics, cybersafety, and cybersecurity at schools,» *International Journal of Cyber Ethics in Education (IJCEE),* τόμ. 4, αρ. 1, pp. 1-15, 2016.

[34] I. Chen και L. Shen, «Cybercitizens at schools,» *Emerging trends in cyber ethics and education,* pp. 91-117, 2019.

[35] H. Chou και C. Chou, «An analysis of multiple factors relating to teachers' problematic information security behavior,» *Computers in Human Behavior,* τόμ. 65, pp. 334-345, 2016.

[36] G. Javidi και E. Sheybani, «K-12 cybersecurity education, research, and outreach,» σε *2018 IEEE Frontiers in Education Conference (FIE)*, 2018.

[37] H. Haseski, «Cyber Security Skills of Pre-Service Teachers as a Factor in Computer-Assisted Education,» *International Journal of Research in Education and Science,* τόμ. 6, αρ. 3, pp. 484-500, 2020.

[38] I. Corradini και E. Nardelli, «Developing digital awareness at school: a fundamental step for cybersecurity education,» σε *International Conference on Applied Human Factors and Ergonomics*, 2020.

[39] E. T. Caparino, «Teachers' Perception on Cyber Security,» *Advanced Science Letters,* τόμ. 24, αρ. 11, pp. 8471-8475, 2018.

[40] S. Al-Janabi και I. AlShourbaji, «A Study of Cyber Security Awareness in Educational Environment in the Middle East,» *Journal of Information & Knowledge Management,* τόμ. 15, p. 1650007, 2016.

[41] M. Al-Tajer και I. Adeyemi, «Cyber Security Threat Awareness Framework for High School Students in Qatar,» 2022.

[42] J. Bustard, «Improving student engagement in the study of professional ethics: concepts and an example in cyber security,» *Science and Engineering Ethics,* τόμ. 24, αρ. 2, pp. 683-698, 2018.

[43] M. Jethwani, N. Memon, W. Seo και A. Richer, «"I Can Actually Be a Super Sleuth" Promising Practices for Engaging Adolescent Girls in Cybersecurity Education,» *Journal of Educational Computing Research,* τόμ. 55, αρ. 1, pp. 3-25, 2017.

[44] Π. Παπαναστασίου και Κ. Ε. Παπαναστασίου, Μεθοδολογία Εκπαιδευτικής Έρευνας, Λευκωσία: Kailas Printers and Lithographers Ltd, 2005.

[45] L. Muniandy, B. Muniandy και Z. Samsudin, «Cyber security behaviour among higher education students in Malaysia,» *J. Inf. Assur. Cyber Secur,* pp. 1-13, 2017.