ΠΑΝΕΛΛΗΝΙΟΣ ΜΑΘΗΤΙΚΟΣ ΔΙΑΓΩΝΙΣΜΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

University of Piraeus
Systems Security Laboratory (SSL)
Department of Digital Systems

HELLENIC CYBER SECURITY TEAM

ΠΡΟΚΗΡΥΞΗ ΓΙΑ ΤΟΝ ΠΑΝΕΛΛΗΝΙΟ ΜΑΘΗΤΙΚΟ ΔΙΑΓΩΝΙΣΜΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Ο **Πανελλήνιος Μαθητικός Διαγωνισμός Κυβερνοασφάλειας (ΠΜΔΚ)** στοχεύει στην αναβάθμιση της επιστήμης της πληροφορικής στην εκπαιδευτική διαδικασία και στην ανάδειξη του ρόλου της στη σύγχρονη ψηφιακή εποχή. Σκοπός του διαγωνισμού είναι η επιλογή και η ανάδειξη ταλαντούχων μαθητών/-τριών της χώρας που ασχολούνται με την κυβερνοασφάλεια (Cybersecurity).

ΦΟΡΕΑΣ ΔΙΟΡΓΑΝΩΣΗΣ ΔΙΑΓΩΝΙΣΜΟΥ

Φορέας διοργάνωσης του διαγωνισμού είναι το Πανεπιστήμιο Πειραιώς και πιο συγκεκριμένα το Τμήμα Ψηφιακών Συστημάτων. Στο Τμήμα Ψηφιακών Συστημάτων λειτουργεί τα τελευταία δεκαοκτώ (18) χρόνια το Πρόγραμμα Μεταπτυχιακών Σπουδών «Ασφάλεια Ψηφιακών Συστημάτων», ενώ το 2008 ιδρύθηκε το Εργαστήριο Ασφάλειας Συστημάτων (SSL), ως μονάδα έρευνας και μεταπτυχιακής εκπαίδευσης.

Από το 2016 το Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς με επικεφαλής τον καθηγητή κ. Χρήστο Ξενάκη φέρει την ευθύνη της Ελληνικής συμμετοχής στον πανευρωπαϊκό διαγωνισμό κυβερνοασφάλειας European Cyber Security Challenge. Ο διαγωνισμός αποτελεί μία πρωτοβουλία του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας ENISA (European Union Agency for Cybersecurity), ενώ υποστηρίζεται ενεργά από το Υπουργείο Ψηφιακής Διακυβέρνησης. Στο πλαίσιο του εν λόγω διαγωνισμού, συγκροτείται κάθε χρόνο η Εθνική Ομάδα Κυβερνοασφάλειας η οποία μέχρι σήμερα έχει καταφέρει να ανταπεξέλθει στις πολύ υψηλές απαιτήσεις της διαγωνιστικής διαδικασίας, αντιμετωπίζοντας επάξια, τεχνολογικά πολύ προηγμένες χώρες.

Στοιχεία Υπευθύνου Επικοινωνίας: Καθηγητής Χρήστος Ξενάκης xenakis@unipi.gr

ΤΙ ΕΙΝΑΙ Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Η σύγχρονη εποχή χαρακτηρίζεται αναμφισβήτητα από την ολοένα αυξανόμενη χρήση του διαδικτύου, κυρίως από τους νέους, αφού οι συναλλαγές, η ενημέρωση, η ψυχαγωγία και η επικοινωνία, συντελούνται κατά κύριο λόγο με ψηφιακά μέσα. Η διευκόλυνση των συναλλαγών, η αμεσότητα της επικοινωνίας και η εύκολη πρόσβαση στην πληροφορία και την ενημέρωση αποτελούν τα σημαντικότερα πλεονεκτήματα του κυβερνοχώρου.

Η αυξημένη, όμως, χρήση του διαδικτύου δεν έχει μόνο θετική πλευρά, μιας και πίσω από τη διαδικτυακή δραστηριότητα συχνά ελλοχεύουν αόρατοι εχθροί. Οι χρήστες μπορεί να αποτελέσουν στόχο υποκλοπής προσωπικών δεδομένων και εκμετάλλευσης, να εκτραπούν σε ψεύτικες ιστοσελίδες ή να γίνουν παραλήπτες μηνυμάτων ηλεκτρονικού ψαρέματος. Επομένως, η ασφάλεια των διαδικτυακών

συναλλαγών αποτελεί παγκόσμια επιταγή και έχει εξελιχθεί σε έναν ταχέως αναπτυσσόμενο χώρο.

Η Κυβερνοασφάλεια (Cyber Security) αποτελεί τη διαδικασία ανίχνευσης, ανάλυσης, πρόβλεψης και πρόληψης των ψηφιακών απειλών. Οι απειλές αυτές πραγματοποιούνται από κακόβουλους τρίτους (hackers) οι οποίοι στοχεύουν να αποκτήσουν πρόσβαση σε πόρους που δεν έχουν τα κατάλληλα δικαιώματα, να καταστρέψουν ευαίσθητες και σημαντικές πληροφορίες, να αποσπάσουν χρήματα από χρήστες ή να διακόψουν τη ροή εργασιών μιας επιχείρησης ή ενός Οργανισμού.

Αποτέλεσμα της διαμορφωθείσας αυτής κατάστασης είναι η αύξηση της ζήτησης για επαγγελματίες στον τομέα της ψηφιακής ασφάλειας. Ολοένα και περισσότεροι νέοι στρέφονται σε Πανεπιστημιακές σπουδές στον εν λόγω τομέα, καθώς και στην απόκτηση περαιτέρω δεξιοτήτων, μέσω της παρακολούθησης Προγραμμάτων Μεταπτυχιακών Σπουδών, σεμιναρίων και σχετικών πιστοποιήσεων, στοχεύοντας σε μία άμεση επαγγελματική αποκατάσταση, με προοπτικές εξέλιξης, σε έναν διαρκώς μεταβαλλόμενο και δελεαστικό κλάδο.

ΟΡΟΙ ΔΙΑΓΩΝΙΣΜΟΥ

Ο διαγωνισμός θα διεξαχθεί κατά το σχολικό έτος 2024-2025 στην εκπαιδευτική βαθμίδα του Λυκείου (Α, Β και Γ τάξη) και όλα τα σχολεία της χώρας, δημόσια και ιδιωτικά, θα έχουν τη δυνατότητα να συμμετάσχουν με ομάδες μαθητών/-τριών μέχρι πέντε (5) ατόμων. Η διεξαγωγή του διαγωνισμού θα πραγματοποιηθεί διαδικτυακά και σε ορισμένο χρόνο, εκτός ωρολογίου προγράμματος, μέσω της πλατφόρμας που έχει ετοιμάσει το Πανεπιστήμιο Πειραιώς ειδικά για τον διαγωνισμό, η οποία είναι βασισμένη στην πλατφόρμα CTFd, την πιο δημοφιλή πλατφόρμα για την οργάνωση, διεξαγωγή και διαχείριση διοργανώσεων τύπου “Πιάσε την Σημαία” (Capture The Flag). Η πλατφόρμα αυτή είναι ανοιχτού κώδικα και χρησιμοποιείται αποκλειστικά για την διεξαγωγή εκπαιδευτικών προγραμμάτων πάνω στην κυβερνοασφάλεια.

Στην εν λόγω πλατφόρμα θα αναρτηθεί ένας αριθμός από ανεξάρτητες δοκιμασίες πάνω στην ψηφιακή ασφάλεια, τις οποίες οι μαθητές/-τριες θα κληθούν να ολοκληρώσουν ανακτώντας την κρυμμένη σημαία της κάθε δοκιμασίας. Με την επιτυχή ολοκλήρωση κάποιας δοκιμασίας και την υποβολή της σημαίας της στην πλατφόρμα, η ομάδα θα λαμβάνει πόντους ανάλογους της δυσκολίας της δοκιμασίας.

Κατά την διάρκεια του διαγωνισμού, μέσω της πλατφόρμας οι υπεύθυνοι καθηγητές, εκπροσωπώντας το συμμετέχον σχολείο, θα μπορούν να αποκτήσουν πρόσβαση στην εκφώνηση και το συνοδευτικό υλικό της κάθε δοκιμασίας, καθώς επίσης και να υποβάλουν τις αντίστοιχες σημαίες/απαντήσεις για την κάθε δοκιμασία με σκοπό την απόδοση των αντίστοιχων πόντων νίκης στην ομάδα τους. Παράλληλα, θα μπορούν να δουν τους συνολικούς πόντους που έχει συλλέξει η ομάδα τους, καθώς επίσης και ποιες από τις δοκιμασίες δεν έχουν ακόμα επιλυθεί.

Οι μαθητές/-τριες μπορούν να σχηματίσουν ομάδα με τον εκπαιδευτικό τους. Μια ομάδα θα αποτελείται από ένα εκπαιδευτικό και έναν (1) έως πέντε (5) μαθητές/-τριες από το ίδιο σχολείο. Οι εκπαιδευτικοί μπορούν να συμμετέχουν σε παραπάνω από μια (1) ομάδες, αλλά οι μαθητές μπορούν να συμμετέχουν μόνο σε μια (1) ομάδα. Ο ρόλος του εκπαιδευτικού είναι καθαρά συμβουλευτικός, ώστε να βοηθήσει και να καθοδηγήσει τους μαθητές. Σε περίπτωση όπου παραπάνω από πέντε (5)

μαθητές/-τριες από το ίδιο σχολείο ενδιαφέρονται να συμμετέχουν στον διαγωνισμό, οι υπεύθυνοι εκπαιδευτικοί μπορούν να σχηματίσουν περισσότερες από μία (1) ομάδες για το σχολείο.

Η συμμετοχή των μαθητών/-τριών είναι προαιρετική, δεν προβλέπεται οποιαδήποτε οικονομική επιβάρυνσή τους για τη διεξαγωγή του διαγωνισμού και απαιτείται η σύμφωνη γνώμη των Γονέων/ Κηδεμόνων για τη συμμετοχή τους. Τυχόν έξοδα μετακίνησης των μαθητών/-τριών για τη συμμετοχή τους στον διαγωνισμό βαρύνουν αποκλειστικά τους ίδιους/-ες.

Δικαίωμα συμμετοχής στον διαγωνισμό έχουν μόνο οι μαθητές/-τριες που φοιτούν στα Γενικά και Επαγγελματικά (Τομέας Πληροφορικής) Λύκεια της χώρας, δημόσια και ιδιωτικά, και ακολουθούν το αναλυτικό πρόγραμμα σπουδών του Γενικού Λυκείου.

Κατά την διάρκεια του διαγωνισμού δεν επιτρέπεται οι ομάδες να μοιράζουν λύσεις για τις δοκιμασίες μεταξύ τους, δεν επιτρέπεται οι συμμετέχοντες να επιτίθενται σε μηχανήματα που δεν αποτελούν μέρος του διαγωνισμού και δεν επιτρέπεται να επιτίθενται σε οποιοδήποτε σύστημα της υποδομής του διαγωνισμού.

Ο φορέας διοργάνωσης (Πανεπιστήμιο Πειραιώς) αναλαμβάνει όλη τη διαδικασία υλοποίησης του διαγωνισμού και θα διασφαλίσει τα προσωπικά δεδομένα και τα πνευματικά δικαιώματα των δημιουργών, σύμφωνα με την κείμενη νομοθεσία.

Κατά την εφαρμογή του ως άνω διαγωνισμού στα σχολεία είναι εξασφαλισμένη η προστασία των προσωπικών δεδομένων των συμμετεχόντων μαθητών/-τριών, εκπαιδευτικών και γονέων (βάσει της ελληνικής και ευρωπαϊκής νομοθεσίας, Ν. 4624/2019, Γενικός Κανονισμός 2016/679 για την Προστασία Δεδομένων-GDPR). Οι μαθητές/-τριες που υποβάλλουν συμμετοχή αποδέχονται τον κανονισμό περί διαχείρισης των προσωπικών δεδομένων τους.

ΣΤΟΧΟΙ ΓΙΑ ΤΟΥΣ ΜΑΘΗΤΕΣ/-ΤΡΙΕΣ

Ο στόχος για τους μαθητές και τις μαθήτριες είναι:

- Η ενημέρωση των μαθητών/-τριών για την ασφάλεια του διαδικτύου και των κυβερνοαπειλών.
- Η αναγνώριση της ανάγκης προστασίας των προσωπικών τους δεδομένων κατά την περιήγησή τους στο διαδίκτυο.
- Η εκπαίδευση των μαθητών/-τριών σε θέματα κενών ασφαλείας του διαδικτύου.
- Η ανάδειξη νέων ταλέντων στο χώρο της κυβερνοασφάλειας.
- Η ανάδειξη των μελλοντικών μελών της Εθνικής Ομάδας Κυβερνοασφάλειας.

ΠΕΡΙΓΡΑΦΗ ΤΩΝ ΠΡΟΚΛΗΣΕΩΝ

Α. ΠΕΡΙΟΧΕΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΠΟΥ ΚΑΛΥΠΤΟΥΝ ΟΙ ΠΡΟΚΛΗΣΕΙΣ

Οι δοκιμασίες (προκλήσεις) που θα κληθούν οι μαθητές/-τριες να επιλύσουν θα καλύπτουν δημοφιλείς περιοχές της κυβερνοασφάλειας, όπως αυτές κατηγοριοποιούνται σε παρόμοιους ευρωπαϊκούς διαγωνισμούς. Επιπλέον, οι δοκιμασίες θα έχουν διαμορφωθεί ειδικά για το διαγωνισμό και θα είναι πλήρως προσαρμοσμένες στις ανάγκες της ηλικιακής ομάδας στην οποία απευθύνονται. Ο βαθμός δυσκολίας των δοκιμασιών θα εκτείνεται από πολύ εύκολες μέχρι και

δύσκολες, με σκοπό την συμμετοχή όλων των μαθητών με ενδιαφέρον στην ασφάλεια υπολογιστών.

1. Κρυπτογραφία (Cryptography)

Δοκιμασίες σχετικές με κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών και απόκρυψη μηνυμάτων. Σκοπός των δοκιμασιών αυτών είναι να παρέχουν στον χρήστη γνώσεις λειτουργίας κρυπτογραφικών αλγορίθμων και αναγνώριση ευπαθειών σε αυτούς.

2. Παγκόσμιος Ιστός (Web)

Δοκιμασίες σχετικές με την λειτουργία και ασφάλεια διαδικτυακών εφαρμογών. Σκοπός των δοκιμασιών αυτών είναι να παρέχουν στον χρήστη γνώσεις λειτουργίας, μηχανισμών αυθεντικοποίησης και ασφάλειας σε ιστοσελίδες και διακομιστές στον παγκόσμιο ιστό.

3. Αντίστροφη Μηχανική (Reverse Engineering)

Δοκιμασίες σχετικές με την ανάλυση εκτελέσιμων προγραμμάτων σε γλώσσα μηχανής. Σκοπός των δοκιμασιών αυτών είναι η κατανόηση λειτουργίας δυαδικών προγραμμάτων και εκτέλεσής τους από το εκάστοτε λειτουργικό σύστημα.

4. Ψηφιακή Εγκληματολογία (Digital Forensics)

Δοκιμασίες σχετικές με την ανάλυση πληροφοριών με σκοπό την αναγνώριση και ανάκτηση ηλεκτρονικών αποδεικτικών στοιχείων. Σκοπός των δοκιμασιών αυτών είναι η παροχή γνώσεων τηλεπικοινωνιών και πρωτοκόλλων, καθώς και μεθόδων ανάλυσής τους για την ανάκτηση πληροφοριών.

5. Εκμετάλλευση αδυναμιών (Pwn/Binary exploitation)

Δοκιμασίες που απαιτούν την εκμετάλλευση αδυναμιών σε εκτελέσιμα αρχεία, οι συμμετέχοντες συνήθως παρέχονται με ένα ευάλωτο δυαδικό πρόγραμμα και τους ζητείται να εντοπίσουν και να εκμεταλλευτούν ευπάθειες μέσα σε αυτό για να αποκτήσουν έλεγχο ή να εξάγουν ευαίσθητες πληροφορίες.

6. Στεγανογραφία (Steganography)

Δοκιμασίες σχετικές με την ανάλυση πληροφοριών και ανάκτηση κρυμμένων μηνυμάτων. Σκοπός των δοκιμασιών αυτών είναι η παροχή γνώσεων πάνω σε τεχνικές στεγανογραφίας, αλλά και τεχνικές κωδικοποίησης πληροφοριών.

7. Συλλογή Πληροφοριών από Ανοιχτές Πηγές (Open Source Intelligence, OSINT)

Δοκιμασίες που απαιτούν την εκμετάλλευση δημόσια διαθέσιμων πληροφοριών για την εύρεση κρυμμένων δεδομένων, λύση προβλημάτων ή εύρεση ευπαθειών. Ο στόχος είναι να αξιοποιηθούν πηγές ανοικτής πληροφορίας όπως δημόσια ιστοσελίδες, μέσα κοινωνικής δικτύωσης, φόρουμ και άλλες δημόσιες πλατφόρμες για την απόκτηση πληροφοριών.

8. Διάφορα (Miscellaneous)

Δοκιμασίες σχετικές με την επίλυση γρίφων και προβλημάτων. Σκοπός των δοκιμασιών αυτών είναι η εκπαίδευση του χρήστη στην επίλυση προβλημάτων, αλλά και η εξοικείωσή του με τεχνολογίες σχετικές με την κυβερνοασφάλεια.

Σκοπός του διαγωνισμού είναι η ευαισθητοποίηση των μαθητών/-τριών του λυκείου σε θέματα κυβερνοασφάλειας και η παροχή σε αυτούς/αυτές γνώσεων

κυβερνοασφάλειας. Επιπλέον, δίνεται η δυνατότητα στους εκπαιδευτικούς να χρησιμοποιήσουν το υλικό του διαγωνισμού για την διεξαγωγή επιπλέον δραστηριοτήτων με τους μαθητές/-τριες με σκοπό την μόρφωσή τους σε θέματα κυβερνοασφάλειας, μιας και μετά το πέρας του διαγωνισμού θα δοθούν αναλυτικές οδηγίες επίλυσης της κάθε δοκιμασίας.

Β. ΕΝΔΕΙΚΤΙΚΕΣ ΠΕΡΙΓΡΑΦΕΣ ΠΡΟΚΛΗΣΕΩΝ

Με σκοπό την ευαισθητοποίηση των μαθητών/-τριών του λυκείου και την παροχή γνώσεων πάνω στην κυβερνοασφάλεια, στο πλαίσιο του Πανελλήνιου Σχολικού Διαγωνισμού Κυβερνοασφάλειας (ΠΜΔΚ) 2025 θα δοθούν στους/στις μαθητές/-τριες μια σειρά από ανεξάρτητες προκλήσεις πάνω στην Κυβερνοασφάλεια.

Για την προετοιμασία τους, οι ενδιαφερόμενοι μαθητές/-τριες μπορούν να δοκιμάσουν να λύσουν τις δοκιμασίες που δόθηκαν στους μαθητές κατά την διεξαγωγή των προηγουμένων Πανελληνίων Μαθητικών Διαγωνισμών Κυβερνοασφάλειας οι οποίες είναι διαθέσιμες στο GitHub του Εργαστηρίου Ασφάλειας Συστημάτων. Μαζί με τις εκφωνήσεις και τα αρχεία των δοκιμασιών αυτών δίνονται και οι ενδεικτικές λύσεις τους, δίνοντας έτσι και την δυνατότητα στους μαθητές/-τριες να ακολουθήσουν βήμα-βήμα την διαδικασία επίλυσής τους ανεξάρτητος του επιπέδου γνώσεων τους στην Κυβερνοασφάλεια.

Ακολουθεί περιγραφή ενδεικτικών προκλήσεων, που μπορεί να κληθούν να επιλύσουν οι μαθητές/-τριες κατά την διάρκεια του διαγωνισμού:

- Ανάκτηση και ανάλυση πηγαίου κώδικα ιστοσελίδων (π.χ. ανάγνωση πηγαίου κώδικα μιας ιστοσελίδας)
- Παράκαμψη αυθεντικοποίησης σε ευπαθής διαδικτυακή εφαρμογή (π.χ. επίθεση με SQL injection σε ιστοσελίδα)
- Ανάκτηση και ανάλυση πηγαίου κώδικα εκτελέσιμων προγραμμάτων με σκοπό την παράκαμψη μηχανισμών ασφαλείας (π.χ. εύρεση κωδικού που ζητά ένα εκτελέσιμο πρόγραμμα)
- Αποκρυπτογράφηση κρυπτογραφημένου μηνύματος με ή χωρίς κλειδί (π.χ. αποκρυπτογράφηση μηνύματος σε Κώδικα του Καίσαρα)
- Ανάλυση και αποκωδικοποίηση μηνυμάτων (π.χ. αποκωδικοποίηση base64)
- Ανάλυση διαδικτυακής ροής (π.χ. ανάλυση ροής πακέτων με Wireshark)
- Σπάσιμο κωδικών (π.χ. ανάκτηση κωδικού σε συμπιεσμένο αρχείο zip)
- Ανάκτηση κρυμμένων μηνυμάτων (π.χ. ανάκτηση μηνύματος από φωτογραφία)
- Εκμετάλλευση ευπαθειών σε κρυπτογραφικά συστήματα (π.χ. εύρεση αδύναμου ιδιωτικού κλειδιού)
- Ανακατασκευή/διόρθωση κατεστραμμένου αρχείου (π.χ. διόρθωση κατεστραμμένης φωτογραφίας)
- Εύρεση δημόσια διαθέσιμων πληροφοριών στο διαδίκτυο (π.χ. εύρεση

λογαριασμού ατόμου σε μέσα κοινωνικής δικτύωσης)

ΟΡΓΑΝΩΣΗ ΤΟΥ ΠΑΝΕΛΛΗΝΙΟΥ ΜΑΘΗΤΙΚΟΥ ΔΙΑΓΩΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (ΠΜΔΚ)

Για τις ανάγκες του διαγωνισμού θα συσταθούν:

Α) Οργανωτική – Επιστημονική Επιτροπή (Ο.Ε.Ε.), η οποία έχει την ευθύνη α) της οργάνωσης και διεξαγωγής του διαγωνισμού, β) της κατάρτισης των διαδικτυακών δοκιμασιών κυβερνοασφάλειας (cybersecurity challenges) που θα κληθούν να επιλύσουν οι διαγωνιζόμενοι και γ) της αξιολόγησης των επιδόσεων της ομάδας και της έκδοσης αποτελεσμάτων. Η ΟΕ απαρτίζεται από έμπειρο διδακτικό/ερευνητικό προσωπικό και Υποψήφιους Διδάκτορες του Πανεπιστημίου Πειραιώς και δεσμεύεται από τον κανονισμό GDPR για τη διαχείριση των δεδομένων που συλλέγει.

ΜΕΛΗ ΟΡΓΑΝΩΤΙΚΗΣ – ΕΠΙΣΤΗΜΟΝΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΔΙΑΓΩΝΙΣΜΟΥ			
Α/Α	**ΟΝΟΜΑΤΕΠΩΝΥΜΟ**	**ΙΔΙΟΤΗΤΑ**	**ΦΟΡΕΑΣ**
1.	Χρήστος Ξενάκης	Καθηγητής, Πρόεδρος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
2.	Αγγελική Πάνου	Ειδικό Διδακτικό Προσωπικό (Ε.ΔΙ.Π.), μέλος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
3.	Αικατερίνη Πούπουζα	Ειδικό Τεχνικό Εργαστηριακό Προσωπικό (Ε.Τ.Ε.Π.), μέλος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
4.	Αριστείδης Φαραώ	Διδάκτορας, μέλος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
5.	Βάιος Μπολγούρας	Υποψήφιος Διδάκτορας, μέλος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
6.	Αθανάσιος – Βασίλειος Γραμματόπουλος	Υποψήφιος Διδάκτορας, μέλος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
7.	Μιχαήλ Τακαρώνης	Μέλος Εργαστηρίου Ασφάλειας Συστημάτων (SSL), μέλος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων

Β) Αξιολογική Επιτροπή (Α.Ε.), η οποία έχει την ευθύνη α) της επιστημονικής εγκυρότητας των δοκιμασιών κυβερνοασφάλειας (cybersecurity challenges) και β) της ένταξης των επιτυχόντων ομάδων στην Εθνική Ομάδα Κυβερνοασφάλειας. Η

Επιστημονική Επιτροπή απαρτίζεται από έμπειρους Καθηγητές και Υποψήφιους Διδάκτορες του Πανεπιστημίου Πειραιώς.

ΜΕΛΗ ΑΞΙΟΛΟΓΙΚΗΣ ΕΠΙΤΡΟΠΗΣ ΔΙΑΓΩΝΙΣΜΟΥ			
Α/Α	**ΟΝΟΜΑΤΕΠΩΝΥΜΟ**	**ΙΔΙΟΤΗΤΑ**	**ΦΟΡΕΑΣ**
1	Χρήστος Ξενάκης	Καθηγητής, Πρόεδρος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
2	Αριστείδης Φαραώ	Διδάκτορας, μέλος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων
3	Αθανάσιος Βασίλειος Γραμματόπουλος	Υποψήφιος διδάκτορας, μέλος Επιτροπής	Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων

Η σύστασή των ανωτέρω επιτροπών θα αναρτηθεί στον ιστότοπο του διαγωνισμού https://ecsc.gr/index.php/panellhnios-mathitikos-diagonismos-kybernoasfaleias/

Ο Πανελλήνιος Μαθητικός Διαγωνισμός Κυβερνοασφάλειας (ΠΜΔΚ) θα διεξαχθεί τον Φεβρουάριο του 2025 για τους μαθητές/-τριες της Α΄, Β΄ και Γ΄ Λυκείου.

Ως ημερομηνία έναρξης εγγραφών των ομάδων στο διαγωνισμό ορίζεται η **02/12/2024** και ως καταληκτική ημερομηνία υποβολής των εγγραφών ορίζεται η **24/01/2025**. Εφόσον ολοκληρωθούν οι εγγραφές, και οι ομάδες λάβουν οδηγίες σχετικά με το πως θα μπουν στην πλατφόρμα και θα παίξουν, οι ομάδες θα μπορούν να μπαίνουν στην πλατφόρμα για να παίξουν τα challenges κατά τις ημερομηνίες **03/02/2025 (ώρα έναρξης: 9:00) έως 03/03/2025 (ώρα λήξης: 15:00)**.

Ο διαγωνισμός δύναται να πραγματοποιηθεί εντός και εκτός ωρολογίου προγράμματος. Στην περίπτωση που επιλεχθεί από τους εκπαιδευτικούς να γίνει η προετοιμασία των μαθητών/-τριών για τη συμμετοχή τους στο διαγωνισμό εντός του ωρολογίου προγράμματος προτείνεται η ώρα του μαθήματος της πληροφορικής, με μέγιστη διάρκεια τις τέσσερις (4) διδακτικές ώρες. Ο εν λόγω διαγωνισμός δεν επιβαρύνει τη διδασκαλία των επιμέρους γνωστικών αντικειμένων του μαθήματος της πληροφορικής, αλλά, αντίθετα εμπλουτίζει την εκπαιδευτική διαδικασία και τους εκπαιδευτικούς στόχους του μαθήματος. Οι μαθητές/-τριες μέσα από την όλη διαδικασία και με βιωματικό τρόπο θα συνεργαστούν, θα αποκτήσουν γνώσεις και θα προσπαθήσουν να αναπτύξουν δεξιότητες για την επίλυση των δοκιμασιών.

Κάθε μαθητής/-τρια υποβάλλει τη δήλωση συμμετοχής του/της γραπτώς στον/στην Διευθυντή/-ντρια του σχολείου, συνοδευόμενη από την έγγραφη συναίνεση γονέα/κηδεμόνα. Τη φόρμα συναίνεσης μπορείτε να τη βρείτε εδώ και **είναι υποχρεωτικό** να υποβληθεί μαζί με την αίτηση συμμετοχής.

Εφόσον υπάρχουν ενδιαφερόμενοι μαθητές/-τριες, ο/η Διευθυντής/-ντρια ορίζει ως υπεύθυνο/-η για το διαγωνισμό έναν/μία εκπαιδευτικό του σχολείου ο/η οποίος/-α

κατά προτίμηση διδάσκει το μάθημα της Πληροφορικής. Ο/η εκπαιδευτικός θα απασχοληθεί εθελοντικά, χωρίς δαπάνη για το Δημόσιο, και θα φροντίσει:

- Να συμπληρώσει, μέχρι την Παρασκευή, 24 Ιανουαρίου 2025, την ηλεκτρονική φόρμα που βρίσκεται εδώ με τα παρακάτω υποχρεωτικά πεδία:
  - Όνομα και Επώνυμο Υπευθύνου Εκπαιδευτικού
  - Email Επικοινωνίας
  - Φορέας (Όνομα Σχολείου ή Οργανισμού)
  - Διεύθυνση Φορέα
  - Υπογεγραμμένη φόρμα συγκατάθεσης γονέα/κηδεμόνα (πρότυπο φόρμας εδώ).
  - Όνομα και επώνυμο μαθητών /-τριών
  - Τάξη
- κατά τη διάρκεια του διαγωνισμού να έχουν όλοι/-ες οι διαγωνιζόμενοι/-ες απρόσκοπτη πρόσβαση στο διαδίκτυο (διάθεση της αίθουσας Πληροφορικής, χρησιμοποίηση laptops του σχολείου ή των μαθητών/-τριών κ.α.)
- την απαραίτητη επιτήρηση των διαγωνιζομένων.

Επίσης, ο/η Διευθυντής/-ντρια φροντίζει για την απαραίτητη αναμόρφωση του ωρολογίου προγράμματος, ώστε να μην διαταραχθεί η ομαλή λειτουργία του σχολείου.

Μετά την λήξη των εγγραφών στον διαγωνισμό, οι εκπαιδευτικοί θα λάβουν ένα όνομα χρήστη και ένα κωδικό για κάθε δηλωθείσα ομάδα και αναλυτικές οδηγίες σχετικά με το πώς και πότε μπορούν να μπουν στην πλατφόρμα και να παίξουν μαζί με τους μαθητές τους τις δοκιμασίες του διαγωνισμού.

ΝΙΚΗΤΗΡΙΕΣ ΟΜΑΔΕΣ ΚΑΙ ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ

Η κατάταξη των ομάδων θα γίνει με βάση την αξιολόγηση των επιδόσεών τους στις δοκιμασίες, λαμβάνοντας υπόψη και τις συνοπτικές εκθέσεις (write-ups) που θα αποστείλουν οι ομάδες. Στις εκθέσεις αυτές θα περιγράφεται η μεθοδολογία που ακολουθήθηκε για την επίλυση της κάθε δοκιμασίας. Από την τελική κατάταξη ενδέχεται να αφαιρεθούν ομάδες οι οποίες δεν πληρούν τους όρους του διαγωνισμού.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΠΟΤΙΜΗΣΗΣ ΤΟΥ ΔΙΑΓΩΝΙΣΜΟΥ

Προβλέπονται διαδικασίες αποτίμησής του διαγωνισμού και υλικό αξιολόγησης το οποίο θα συμπληρώνεται προαιρετικά από τους/τις εκπαιδευτικούς. Τη φόρμα αξιολόγησης μπορούν οι εκπαιδευτικοί να την δουν εδώ και να την συμπληρώσουν μετά την λήξη του διαγωνισμού.

ΒΡΑΒΕΙΑ – ΕΠΑΙΝΟΙ

Οι μαθητές/-τριες των ομάδων που θα κατακτήσουν την 1η, τη 2η και την 3η θέση θα βραβευτούν και θα έχουν την ευκαιρία να συμμετάσχουν στις προπονήσεις της Εθνικής Ομάδας Κυβερνοασφάλειας, στο πλαίσιο της προετοιμασίας της για τον **πανευρωπαϊκό διαγωνισμό European Cyber Security Challenge (ECSC)**. Σε όλα τα μέλη

των ομάδων που θα συμμετάσχουν στο διαγωνισμό θα χορηγηθεί βεβαίωση συμμετοχής.