



**ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΓΡΑΦΕΙΟ ΤΥΠΟΥ**

Τηλ. 2310 997158 e-mail: press@auth.gr

Κτίριο Διοίκησης «Κ. Καραθεοδωρή» ΑΠΘ, Τ.Κ. 541 24, Θεσσαλονίκη

[@Aristoteleio](https://www.facebook.com/Aristoteleio) [@auth_university_thessaloniki](https://www.instagram.com/auth_university_thessaloniki) [@Auth_University](https://twitter.com/Auth_University)

ΔΕΛΤΙΟ ΤΥΠΟΥ

**COCOON: Το ΑΠΘ θωρακίζει τα Ηλεκτρικά Δίκτυα από
Κυβερνοαπειλές**

Θεσσαλονίκη, 17/3/2025

Στο πλαίσιο του καινοτόμου ευρωπαϊκού ερευνητικού προγράμματος COCOON, το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του ΑΠΘ διοργανώνει, την Παρασκευή 21 Μαρτίου 2025 και ώρα 10.00, ένα εξειδικευμένο workshop για την κυβερνοασφάλεια των ηλεκτρικών δικτύων.

Αντικείμενο του ερευνητικού προγράμματος COCOON (Cooperative Cybersecurity for Modern Power Grids-Συνεργατική Κυβερνοασφάλεια Σύγχρονων Ηλεκτρικών Δικτύων) είναι η ενίσχυση της προστασίας των κρίσιμων ενεργειακών υποδομών απέναντι στις αυξανόμενες κυβερνοαπειλές.

Η Σημασία της Κυβερνοασφάλειας στα Ηλεκτρικά Δίκτυα

Η κυβερνοασφάλεια στα ηλεκτρικά δίκτυα είναι σημαντική επειδή αυτά ανήκουν στις λεγόμενες «κρίσιμες υποδομές» και γίνεται επιτακτική και επίκαιρη, καθώς αυξάνεται η διείσδυση Ανανεώσιμων Πηγών Ενέργειας (ΑΠΕ) και συστημάτων αποθήκευσης ηλεκτρικής ενέργειας και επομένως η απαίτηση σε απομακρυσμένο έλεγχο και παρακολούθηση.

Το εύρος και η κλίμακα των πιθανών κυβερνοεπιθέσεων ποικίλει, από αλλοίωση μετρήσεων με στόχο τη διαφοροποίηση χρεώσεων παραγωγής/κατανάλωσης ηλεκτρικής ενέργειας μέχρι συντονισμένη στρέβλωση και παραποίηση εντολών τηλεχειρισμού, με στόχο την ολική αποσταθεροποίηση ή και κατάρρευση του ηλεκτρικού δικτύου. Σε διεθνές επίπεδο, είναι ήδη καταγεγραμμένες αρκετές επιτυχείς, αλλά και πολλές ανεπιτυχείς, κυβερνοεπιθέσεις σε δίκτυα ηλεκτρικής ενέργειας και φυσικού αερίου. Οι επιτυχές επιθέσεις βασίσθηκαν σε κενά και τρωτά σημεία που δημιουργήθηκαν κατά την ψηφιακή μετάβαση των δικτύων ενέργειας.

«Το COCOON, ως ερευνητικό πρόγραμμα και πρόγραμμα καινοτομίας, υλοποιεί αποτελεσματικές παρεμβάσεις για να καλύψει πολλά από αυτά τα κενά, μέσω της συνεργασίας, σε πραγματικό χρόνο, ψηφιακών τεχνικών και μεθόδων ανάλυσης της λειτουργίας των ηλεκτρικών δικτύων, ιδιαίτερα των μελλοντικών δικτύων διανομής ηλεκτρικής ενέργειας» αναφέρει ο Επιστημονικός υπεύθυνος του έργου COCCON, Καθηγητής Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του ΑΠΘ Χάρης Δημουλιάς.

Μία από τις καινοτομίες, η οποία έχει ήδη υλοποιηθεί στον ενάμιση χρόνο που αναπτύσσεται το Cocoon, είναι η ανάλυση και εκτίμηση της φυσικής κατάστασης και των επιτρεπτών ορίων εύρυθμης λειτουργίας ενός ηλεκτρικού δικτύου, καθώς και η εισαγωγή της στις ψηφιακές τεχνικές ως επιπρόσθετη ασπίδα σε κυβερνοεπιθέσεις.

Συγκεκριμένα, τα αποτελέσματα του προγράμματος δοκιμάζονται σε πραγματικές συνθήκες σε τέσσερις πιλοτικές τοποθεσίες στην Ελλάδα, την Ισπανία και την Ολλανδία: Σε μια ενεργειακή κοινότητα στην Χαλκιδική, με την ενεργή συμμετοχή του ΔΕΔΔΗΕ, στο κέντρο ελέγχου δικτύων νοτιοανατολικής Ευρώπης SELENE CC στη Θεσσαλονίκη, σε μεγάλα φωτοβολταϊκά πάρκα στη Σεβίλλη (Ισπανία) και σε ψηφιοποιημένους ηλεκτρικούς υποσταθμούς στο Ντελφτ (Ολλανδία).

Όλες οι πρόσφατες εξελίξεις και βέλτιστες πρακτικές στην κυβερνοασφάλεια των ενεργειακών δικτύων

Το workshop θα φιλοξενήσει διακεκριμένους ομιλητές από την Ελλάδα και το εξωτερικό, οι οποίοι θα αναλύσουν τις τελευταίες εξελίξεις και τις βέλτιστες πρακτικές στον τομέα της κυβερνοασφάλειας των ενεργειακών δικτύων. Μεταξύ των ομιλητών θα είναι ο κ. Μιχάλης Μπλέτσας, Διοικητής της Εθνικής Αρχής για την Κυβερνοασφάλεια, ο οποίος θα αναφερθεί στις τρέχουσες προκλήσεις και τις στρατηγικές για την κυβερνοασφάλεια, εκπρόσωπος του ENISA (European Union Agency for Cybersecurity), που θα παρουσιάσει τις ευρωπαϊκές πρωτοβουλίες για την ασφάλεια κρίσιμων υποδομών, εταίροι του προγράμματος COCOON από τα πανεπιστήμια Κύπρου, Σεβίλλης και Ντελφτ, οι οποίοι θα μοιραστούν λύσεις για την προστασία ενεργειακών κοινοτήτων, πάρκων ΑΠΕ και ψηφιοποιημένων υποσταθμών.

Το workshop θα πραγματοποιηθεί στο κτίριο Δ' της Πολυτεχνικής Σχολής του ΑΠΘ, ενώ θα υπάρχει και δυνατότητα απομακρυσμένης παρακολούθησης μέσω διαδικτύου. Το workshop απευθύνεται σε ερευνητές, επαγγελματίες του κλάδου της ενέργειας και της κυβερνοασφάλειας, καθώς και φορείς χάραξης πολιτικής.

Η συμμετοχή είναι δωρεάν, αλλά απαιτείται εγγραφή μέσω της ιστοσελίδας του προγράμματος COCOON: <https://www.cyber-cocoon.eu/project-event/2388/>. Η γλώσσα του workshop είναι η αγγλική.

Το COCCON, με χρηματοδότηση: 5,2 εκ. ευρώ από το πρόγραμμα Horizon Europe της Ευρωπαϊκής Ένωσης, ξεκίνησε τον Σεπτέμβριο του 2023 και αναμένεται να ολοκληρωθεί τον Σεπτέμβριο του 2026.

Περισσότερες πληροφορίες για το COCCON: <https://www.cyber-cocoon.eu/>

Με την παράκληση να δημοσιευθεί ή να μεταδοθεί και να καλυφθεί η εκδήλωση