หลักสูตร Quantum Technologies and Cybersecurity in the Post-Quantum Era

ระดับ : Intermediate

ระยะเวลาอบรม : 2 วัน

จำนวนผู้เข้าอบรม : 20 คน

วัตถุประสงค์:

1. เข้าใจหลักการพื้นฐานของควอนตัมคอมพิวติงที่แตกต่างจากคอมพิวเตอร์แบบดั้งเดิม
2. ตระหนักถึงภัยคุกคามที่เกิดจากควอนตัมคอมพิวเตอร์ต่อระบบความปลอดภัยในปัจจุบัน
3. เรียนรู้และเข้าใจแนวทางการป้องกันด้วย Post-Quantum Cryptography (PQC) และ Quantum Key Distribution (QKD)
4. สามารถเริ่มต้นใช้งานเครื่องมือและแพลตฟอร์มควอนตัมเบื้องต้นได้

คุณสมบัติผู้เข้าอบรม:

- นักวิทยาการคอมพิวเตอร์, วิศวกรซอฟต์แวร์, วิศวกรเครือข่าย, และผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์

หัวข้อวิชา:

- Introduction to the Quantum Revolution บทนำสู่การปฏิวัติควอนตัม
- Qubits – Superposition คิวบิตและสถานะซ้อนทับ
- Entanglement – Quantum Gates การพัวพันควอนตัมและประตูควอนตัม
- Building Quantum Circuits การสร้างวงจรควอนตัม
- Game-Changing Algorithms อัลกอริทึมพลิกเกมในโลกควอนตัม
- Qubit Technology and Performance เทคโนโลยีคิวบิตและสมรรถนะการทำงาน
- Quantum Transpiler ตัวแปลงวงจรควอนตัม (Quantum Transpiler)
- Quantum Neural Networks เครือข่ายประสาทเทียมเชิงควอนตัม
- Quantum Boltzmann Machines เครื่องโบลต์ซมันน์ ควอนตัม
- Quantum Transformers ทรานส์ฟอร์เมอร์ส ควอนตัม
- Physical Reality – Current Landscape สภาพจริงของเทคโนโลยีควอนตัมและสถานการณ์ปัจจุบัน
- Quantum Threat to Modern Cryptography ภัยคุกคามจากควอนตัมต่อการเข้ารหัสยุคปัจจุบัน
- Post-Quantum Cryptography (PQC) การเข้ารหัสที่ปลอดภัยจากควอนตัม (PQC)

หลักสูตร Quantum Technologies and Cybersecurity in the Post-Quantum Era

- PQC Algorithm Families กลุ่มอัลกอริธึมเข้ารหัสหลังยุคควอนตัม
- Quantum Key Distribution (QKD) การแจกจ่ายกุญแจควอนตัม (QKD)
- Migration to Quantum-Resistant Systems การเปลี่ยนผ่านสู่ระบบต้านทานควอนตัม
- Future Outlook, Strategy – Wrap-up แนวโน้มในอนาคต กลยุทธ์ และการสรุปบทเรียน

วิธีการอบรม : บรรยายและฝึกปฏิบัติ

เกณฑ์การประเมินผล : จำนวนเวลาเข้ารับการอบรมไม่ต่ำกว่า 80% และคะแนนสอบมากกว่า 60%