UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM
Přírodovědecká fakulta

Katedra fyziky Vás zve na přednášku

Dlouhodobá důvěryhodnost elektronických dokumentů v éře kvantových počítačů

Jaroslav Hercík

ze společnosti **Quantalock s.r.o.**

Kdy: čtvrtek **16. dubna 2026 od 13 h**

Kde: aula 1.01, budova CPTO

Anotace:

Při debatách o kvantových počítačích se pozornost často soustředí na šifrovanou komunikaci. Budoucí kvantové hrozby ale dopadají také na dlouhodobou důvěru v elektronické dokumenty. Přednáška ukáže praktické souvislosti pro digitální podpisy, časové ukotvení i integritu dokumentů. Představí aktuální stav vývoje kvantových počítačů a vysvětlí význam Shorova algoritmu pro bezpečnost dnes používaných asymetrických kryptografických systémů. Dále se zaměří na elektronické podpisy a časová razítka, jejich matematické principy a jejich význam pro důvěryhodnost elektronických dokumentů v rámci nařízení eIDAS. Pozornost bude věnována bezpečnostním rizikům, která mohou kvantové počítače přinést v oblasti elektronických podpisů a dlouhodobého časového ukotvení dokumentů. V závěrečné části budou stručně představeny hash-based systémy a Merkleův strom jako možné principy dlouhodobě odolnějšího řešení.

Zve Vás Mgr. Stanislav Pařez, Ph.D.
vedoucí semináře