# NÚKIB připravil podpůrné materiály pro ochranu před hrozbou v podobě kvantových počítačů

**21.7.2023 - | Národní úřad pro kybernetickou a informační bezpečnost**

**Prvním materiálem je přehledový dokument „Útoky s využitím kvantového počítače mohou prolomit současné šifrování: řešením je včasná a efektivní implementace nových standardů“, popisující na manažerské úrovni povahu hrozby kvantových počítačů, časové horizonty, kdy je možné hrozbu očekávat, a základní principy, jak se jí bránit.**

Druhý materiál s názvem *„Minimální požadavky na kryptografické algoritm*y“ jednak aktualizuje minimální požadavky na současné kryptografické algoritmy a zároveň přináší přehled šifrovacích standardů a postupů, které NÚKIB doporučuje používat v následujících letech. Oproti minulým rokům si tento materiál rovněž klade za cíl podporu přípravy přechodu k používání kvantově odolné kryptografie v oblasti kybernetické bezpečnosti.

Třetím materiálem je příloha „Kvantová hrozba a kvantově odolná kryptografie“, jejímž smyslem je informačně doplnit dokument Minimální požadavky na kryptografické algoritmy s bližším zdůvodněním uvedených kryptografických doporučení.

https://www.nukib.cz/cs/infoservis/aktuality/1984-nukib-pripravil-podpurne-materialy-pro-ochranu-pred-hrozbou-v-podobe-kvantovych-pocitacu