**Доповідь: “Концепція зниження ризиків для вразливих криптографічних систем, розробка, стандартизація та впровадження стійких постквантових криптопримітивів на міжнародному та національному рівнях”**


РЕФЕРАТ

*Об’єкт дослідження* – процеси зниження ризиків для вразливих (існуючих) криптографічних систем, розробка, стандартизація та впровадження стандартизованих стійких постквантових криптопримітивів асиметричного шифрування (АСШ), електронного підпису (ЕП) та протоколів інкапсуляції ключів (ПІК) на міжнародному та національному рівнях.

*Предмет досліджень* – методи синтезу та методики оцінки, порівняльного аналізу та застосування нових доказово стійких національних та міжнародних стандартизованих криптографічних примітивів асиметричного шифрування, електронного підпису та протоколів інкапсуляції ключів на міжнародному та національному рівнях.

*Метою доповіді є:*

- обґрунтування вибору, розробка та експериментальні дослідження сучасних та постквантових стандартизованих криптографічних перетворень АСШ, ПІК та ЕП для криптографічного захисту інформації (повідомлень) в мережах зв’язку, надання користувачам мережі зв’язку послуг ідентифікації, автентифікації, цілісності, конфіденційності, доступності, неспростовності, криптографічної живучості та санкціонування кожному користувачу доступу в мережі зв’язку;

- аналіз стану процесів міжнародної стандартизації та умов впровадження асиметричної постквантової криптографії згідно 3-го етапу NIST США та проміжних постквантових та квантових досліджень Європейського союзу (ЄС);

- аналіз стану процесів національної стандартизації та умов і вимог щодо впровадження постквантової асиметричної та симетричної криптографії в Україні, порівняльний аналіз постквантових національних та міжнародних стандартів та проектів стандартів АСШ, ЕП, ПІК згідно вимог щодо безпеки, продуктивності та експлуатаційних характеристик;

- теоретичне обґрунтування та розробка комплексної моделі безпеки та комплексної методики оцінки та порівняльного аналізу постквантових асиметричних криптопримітивів АСШ, ЕП та ПІК згідно вимог щодо безпеки, продуктивності та експлуатаційних характеристик, в умовах класичних та квантових атак та оцінка ризиків від них;

- обґрунтування та розробка структурної схеми, вибір існуючих національних та міжнародних постквантових стандартизованих протоколів та алгоритмів криптографічного захисту інформації в мережах зв’язку;

- результати практичної реалізації систем криптографічного захисту інформації та результати експериментальних досліджень мережі зв’язку на основі використання стандартизованих криптопротоколів АСШ/ПІК, ЕП тощо.

*Методи дослідження* – методи теоретичної та практичної криптології, математичні методи експертного оцінювання та порівняння, методи математичного та програмного моделювання криптографічних перетворень типу АСШ, ЕП, ПІК.