ВИСНОВОК

наукового керівника дисертації **Кандій Сергія Олеговича**
«Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак», поданої на здобуття ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Здобувач наукового ступеня доктора філософії Кандій Сергій Олегович в 2020 році закінчив факультет комп'ютерних наук Харківського національного університету імені В. Н. Каразіна зі здобутою кваліфікацією ступінь вищої освіти магістр, спеціальність «Кібербезпека». Результати, одержані в рамках дисертаційної роботи, є узагальненням багаторічної наукової праці здобувача, у тому числі отримані при виконанні планових науково-дослідних робіт. Здобувач був виконавцем 5 науково-дослідних робіт, тісно пов'язаних з державними і галузевими програмами і планами наукової діяльності. Це дозволило набувати багатого досвіду виконання і впровадження наукових досліджень в області забезпечення криптографічного захисту інформації. Основна увага досліджень була зосереджена на криптографічних перетвореннях на решітках.

Дисертаційна робота виконана самостійно і не містить плагіату.

Ступінь актуальності, глибини і обґрунтованості дисертаційних досліджень дозволяють судити про здібності здобувача самостійно формулювати і вирішувати наукові і прикладні проблеми на відповідному рівні. Аналіз роботи здобувача підтверджує його компетентність в питаннях володіння сучасною методологією наукових досліджень, свідчать про досконалі навики роботи з літературою, умінні критично оцінювати стан і перспективи наукових досліджень у вибраній області.

На першому етапі роботи були детально розглянуті та розкриті вимоги до квантово-стійкої криптографії. Розкрита сутність доказової безпеки та моделей безпеки IND-CCA (Indistinguishability under Adaptive Chosen Chiphertext Attack) для механізмів

інкапсуляції ключів та EUF-CMA (Existentially unforgeable under adaptive chosen message attacks) для електронних підписів.

На другому етапі роботи було обґрунтовано, що фактор Ерміта відіграє важливу роль при аналізі моделей редукції решіток. Проведено серію експериментів, що направлені на визначення точності існуючих асимптотичних оцінок фактору Ерміта на криптографічно значущих розмірностях решіток. Показано, що істинне значення фактору Ерміта швидко наближається до асимптотичних оцінок і на криптографічно значущих розмірностях можливо вважати помилку апроксимації фактору Ерміта незначною. Проведено порівняльний аналіз існуючих симуляторів редукції решіток.

Третій етап роботи був присвячений аналізу існуючих атак на криптографічні перетворення на решітках. Для атак вкладення та декодування була запропонована удосконалена модель оцінки складності атаки, що базується на проведеному у другому розділі аналізі. Для атак декодування запропонований метод визначення оптимальних параметрів атаки. Для криптографічної проблеми SIS запропонована удосконалена модель оцінки складності, що враховує можливість різних значень евклідової норми шуканого вектору.

На четвертому етапі роботи було уточнено оцінки захищеності механізмів інкапсуляції ключів ДСТУ 8961:2019 та Crystals-Kyber. Показано, що врахування структури алгебраїчних решіток дає більші оцінки безпеки, ніж класична модель GSA. Для ДСТУ 8961:2019 отримано доказ IND-CCA безпеки у моделі квантового випадкового оракула.

На п'ятому етапі роботи для електронного підпису Falcon досліджено вплив використання плаваючої точки на безпеку. Запропонована атака відновлення ключів та отримані оцінки необхідної кількості підписів для успішної атаки.

Результати дисертаційних досліджень впровадженні у Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків та були використані при обчисленні вхідних та вихідних тестових векторів стандартів ДСТУ 8961:2019, ДСТУ 9212:2023.

У процесі роботи над дисертацією Кандій С.О. продемонстрував високу цілеспрямованість, наполегливість і працездатність, які дозволили одержати ряд суттєвих результатів. Основні результати, одержані в роботі та безпосередньо і побічно пов'язані з ними, в достатній мірі опубліковані. У тому числі з них: 7 статей у фахових виданнях України, 3 статі у зарубіжних виданнях (індексуються у Scopus, Web of Science), 4 матеріали та тези доповідей на конференціях. Основні теоретичні і практичні результати одержані автором самостійно, про що свідчать опубліковані роботи.

Наведена характеристика професійних якостей здобувача, а також аналіз одержаних їм результатів дозволяють констатувати завершеність досліджень з вибраного науково-прикладного завдання. Рівень підготовленості, досвід наукової роботи Кандій С.О. є підставою для того, щоб рекомендувати до захисту дисертаційну роботу у разовій спеціалізованій вченій раді.

Науковий керівник,
доктор технічних наук, професор кафедри
безпеки інформаційних систем і технологій
Навчально-наукового інституту
комп'ютерних наук та штучного інтелекту
Харківського національного університету
імені В. Н. Каразіна Іван ГОРБЕНКО

Підпис Івана Горбенко засвідчую:
Начальник відділу кадрів
Харківського національного університету
імені В.Н. Каразіна Олена ГРОМИКО