ВИСНОВОК

наукового керівника дисертації **Каптьола Євгенія Юрійовича** «**Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу**», поданої на здобуття ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Здобувач наукового ступеня доктора філософії Каптьол Євгеній Юрійович в 2019 році закінчив факультет комп'ютерних наук Харківського національного університету імені В. Н. Каразіна зі здобутою кваліфікацією ступінь вищої освіти «магістр» за спеціальністю «Кібербезпека». Результати, одержані в рамках дисертаційної роботи є узагальненням багаторічної наукової праці здобувача, у тому числі отримані при виконанні планових науково-дослідних робіт. Основна увага досліджень була зосереджена на методах оцінки та порівняльного аналізу існуючих та перспективних криптографічних перетворень типу асиметричний електронний підпис.

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 було проаналізовано основні вимоги до застосування та оцінки існуючих та перспективних асиметричних

криптоперетворень в умовах перехідного періоду та підготовки до настання постквантового періоду, для яких характерним є здійснення як класичних так і квантових атак. Проведений аналіз дозволив сформулювати мету, об'єкт, предмет і задачі дослідження.

На другому етапі роботи було досліджено особливості та варіанти практичного застосування криптографічних перетворень типу асиметричний електронний підпис. Також було обгрунтовано та розроблено моделі загроз, порушника та безпеки, актуальних для оцінки існуючих та перспективних асиметричних електронних підписів в перехідний та постквантовий періоди. Було обгрунтовано категорії та показники оцінки криптографічної стійкості існуючих та перспективних криптографічних перетворень, за умови застосування систем безумовних, умовних та прагматичних критеріїв.

Третій етап роботи був присвячений обгрунтованню та розробці методичних основ та методики оцінки криптографічної стійкості асиметричних криптоперетворень на основі існуючих методів криптоаналізу. Обгрунтовано комплексну методику оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу, та запропоновано вдосконалення комплексної методики оцінки та порівняльного аналізу в частині врахування в процесі оцінки та порівняння за прагматичними критеріями мети здійснення порівняння та можливих варіантів застосування ЕП, що призодить до збільшення точності та відповідності отриманого результату вихідним вимогам.

На четвертому етапі роботи було отримано оцінки та порівняння стійкості як кандидатів на стандартизацію, так і вже стандартизованих для використання в перехідний та пост-квантовий періоди алгоритми електронного підпису. Проведено порівняння отриманих результатів порівняння вже стандартизованих алгоритмів з міжнародними результатами,

що вказує на те, що обрані математичні методи здійснення квантового криптоаналізу є актуальними для застосування в оцінці та порівнянні стійкості асиметричних криптографічних перетворень як для класичного, так і квантового комп'ютера. Надано відповідні оцінки та порівняння, що дозволяють обрати такі криптографічні перетворення, що забезпечують виконання вимог.

На п'ятому етапі роботи уточнено оцінки та отримано експерементальні результати порівняння електронних підписів за допомогою розробленої моделі модифікації комплексної методики оцінки та порівняння. Отримані значення продемонстрували ефективність розроблених методів та моделей. Для електронного підпису Falcon запропонована атака відновлення ключів. Сформульовано та обгрунтовано практичні рекомендації щодо перекриття вразливостей електронного підпису Falcon до наведеної атаки.

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

У процесі роботи над дисертацією Каптьол Є. Ю. проявив себе працелюбним, вдумливим дослідником з широкою науковою ерудицією та аналітичними здібностями. Він продемонстрував здатність пошуку, обробки та використання великих об'ємів науково-технічної інформації в тому числі на англійській мові, вміння чітко ставити, формулювати та вирішувати складні наукові завдання; публікувати результати досліджень у міжнародних та українських фахових виданнях, доповідати їх на наукових конференціях та семінарах.

Основні результати, одержані в роботі та безпосередньо і побічно пов'язані з ними, в достатній мірі опубліковані. У тому числі з них: 4 статті у фахових виданнях України, 2 статті у зарубіжних виданнях (індексуються у

Scopus, Web of Science), 5 матеріалів та тез 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 Каптьол Є.Ю. 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