ЗАТВЕРДЖЕНО
Наказ Міністерства освіти і науки України
__ _____ 202_ року № _____

Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач (ка) ступеня доктора філософії __Кандій Сергій Олегович_____,
(власне ім'я, прізвище здобувача (ки))
_1997__ року народження, громадянин (ка) __України_____,
(назва держави, громадянином якої є здобувач (ка))
освіта вища: закінчив (ла) у _2020___ році _Харківський національний університет імені В.Н. Каразіна_____
(найменування закладу вищої освіти)
за спеціальністю (спеціальностями) __Кібербезпека_____
(за дипломом)
_____,
працює науковим співробітником-консультантом____ в __ПрАТ «ІІТ»_____,
(посада) (місце основної роботи, підпорядкування, місто)
виконав (ла) акредитовану освітньо-наукову програму **Кібербезпека**.
Разова спеціалізована вчена рада, утворена наказом Харківського національного університету
(повне найменування закладу вищої освіти
імені В.Н. Каразіна Міністерством освіти та науки України, м. Харків_____
від **«3» квітня 2025 року № 0114-1/173**
(наукової установи), підпорядкування (у родовому відмінку), місто)
зі змінами (за наявності), внесеними наказом від «___» _____ 20__ року № _____, у складі:
Голови разової спеціалізованої вченої ради - _Єсіна Віталія Івановича, доктора технічних наук, професора, професора кафедри кібербезпеки інформаційних систем, мереж і технологій Навчального-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна,_____
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Рецензентів - _Олійникова Романа Васильовича, доктора технічних наук, професора, професора кафедри кібербезпеки інформаційних систем, мереж і технологій Навчального-наукового інституту комп'ютерних наук а штучного інтелекту Харківського національного університету імені В. Н. Каразіна,_____
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Офіційних опонентів - Толюпи Сергія Васильовича, доктора технічних наук, професора, професора кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка,_____
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Чевардіна Владислава Євгенійовича, доктора технічних наук, професора, начальника кафедри кібербезпеки військового інституту телекомунікацій та інформатизації імені Героїв Крут,_____
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Корченко Олександра Григоровича, доктора технічних наук, професора, першого проректора державного університету інформаційно-комунікаційних технологій,_____
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
на засіданні «2» ___червня____ 2025_ року прийняла рішення про присудження ступеня доктора філософії з галузі знань _12 Інформаційні технології_____
(галузь знань)
_____Кандію Сергію Олеговичу_____

(власне ім'я, прізвище здобувача (ки) у давальному відмінку)

на підставі публічного захисту дисертації «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак»

(назва дисертації)

за спеціальністю (спеціальностями) 125 Кібербезпека та захист інформації

(код і найменування спеціальності (спеціальностей)

.

відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Дисертацію виконано у (в) Харківському університеті імені В.Н. Каразіна, Міністерство освіти і науки України, м. Харків

(найменування закладу вищої освіти (наукової установи), підпорядкування, місто)

Науковий керівник (керівники) Горбенко Іван Дмитрович, доктор технічних наук, професор, професор кафедри кібербезпеки інформаційних систем, мереж і технологій Навчального-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна

(власне ім'я, прізвище, науковий ступінь, вчене звання, місце роботи, посада)

Дисертацію подано у вигляді спеціально підготовленого рукопису (наводиться аналіз дисертації щодо дотримання вимог пункту 6 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами)).

Здобувач (ка) має 16 наукових публікацій за темою дисертації, з них 10 (наводиться аналіз наукових публікацій щодо дотримання вимог пунктів 8, 9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії) (зазначити наукові публікації):

1. Gorbenko I.D., Yesina M.V., Kandy S.O., Ostryanska Ye. V. Generation of general system parameters for Falcon cryptosystem for 256, 384, and 512 security bits // Telecommunications and Radio Engineering. 2022. Vol. 81, Is. 2. P. 49–59. https://www.dl.begellhouse.com/journals/0632a9d54950b268,33bd45d917452b68,54c5c714496ce4ca.html DOI:10.1615/TelecomRadEng.2022037071.

2. Potii O.V., Kachko O.G., Kandii S.O., Kaptol Y.Y. Determining the effect of a floating point on the Falcon Digital Signature Algorithm Security // Eastern–European Journal of Enterprise Technologies. 2024. Vol. 1, Is. 9. P. 52–59. https://journals.uran.ua/eejet/article/view/295160 DOI:10.15587/1729–4061.2024.295160.

3. Kachko O.G., Gorbenko Y.I., Kandii S.O., Kaptol Y.Y. Improving protection of falcon electronic signature software implementations against attacks based on Floating Point Noise // Eastern–European Journal of Enterprise Technologies. 2024. Vol. 4, Is. 9, P. 6–17. https://journals.uran.ua/eejet/article/view/310521 DOI:10.15587/1729–4061.2024.310521

4. Gorbenko Yu.I., Kandii S.O. Comparison of security arguments of promising key encapsulation mechanisms // Radiotekhnika. 2022. Vol. 210. P. 22–36. http://rt.nure.ua/article/view/268561/264140 DOI:10.30837/rt.2022.3.210.02

5. Kandiy S.O. Analysis of DSTU 8961:2019 in random Oracle Model // Radiotekhnika. 2022. Vol. 211. P. 22–36. http://rt.nure.ua/article/view/278028 DOI:10.30837/rt.2022.4.211.02

6. Kandiy S.O., Ostrianska Ye.V., Gorbenko I.D., Yesina M.V. Classification and analysis of vulnerabilities of modern information systems from classical and quantum attacks. Radiotekhnika. 2022. Vol. 211. P. 7–21. http://rt.nure.ua/article/view/278027 DOI: 10.30837/rt.2022.4.211.01

7. Kandiy S.O., Gorbenko I.D. Security analysis of promising key encapsulation mechanisms in the core–SVP model // Radiotekhnika. 2023. Vol. 212. P. 66–84. http://rt.nure.ua/article/view/286564 DOI:10.30837/rt.2023.1.212.06

8. Kandii S.O., Gorbenko I.D. Analysis of DSTU 8961:2019 in the quantum random Oracle Model // Radiotekhnika. 2023. Vol. 214. P. 7–16. http://rt.nure.ua/article/view/297798/290701 DOI:10.30837/rt.2023.3.214.01

9. Kandii S.O., Gorbenko I.D. Refinement of security estimates of quantum–resistant standards of asymmetric encryption taking into account the structure of q–arry lattices // Radiotekhnika. 2024. Vol 218. P. 76–92. http://rt.nure.ua/article/view/318798/309118 DOI:10.30837/rt.2024.3.218.06

10. Kandii S.O., Gorbenko I.D. Assessing the influence of the algebraic structure of q–ary lattices on the complexity of cryptanalysis of problems on lattices // Radiotekhnika. 2024. Vol. 217. P. 79–99. http://rt.nure.ua/article/view/310856 DOI:10.30837/rt.2024.2.217.07.

У дискусії взяли участь (голова, рецензенти, офіційні опоненти, інші присутні) та висловили зауваження:

Олійников Р.В.

1) Метрика середньоквадратичної помилки, що використовується для оцінки якості роботи моделей редукції решіток, оцінює лише "середній" сценарій. У криптографії критичні саме гірші випадки. У роботі не показано, чи не приховують усереднені цифри окремі, але небезпечні для безпеки аномалії профілю базису.

2) Формула (3.9) базується на припущенні нормального розподілу таємного вектора, тоді як у гібридній атаці використовуються інші розподіли. Автор сам зауважує цю невідповідність, але пропонує лише апроксимацію, не перевіряючи похибку такої заміни на безпеку.

3) Роботі бракує порівняльного тестування з альтернативними оцінками точності роботи симуляторів редукції решіток. Хоча автор наводить власні симуляції, відсутнє пряме зіставлення з незалежними цифрами, що обмежує зовнішню валідацію висновків.

Толюпа С.В.

1) У роботі наведено ґрунтовний теоретичний аналіз криптографічних схем, проте не показано, як отримані наукові результати трансформуються у практичні рекомендації чи безпосереднє вдосконалення реальних протоколів і стандартів.

2) Оцінка складності атак вкладення значною мірою спирається на евристику (критерій (3.2) та ймовірність відновлення (3.3)). Хоча ці евристики добре зарекомендували себе на практиці, відсутність строгих доведень є слабким місцем. Варто було б зазначити цю обмеженість.

3) Відсутні приклади інтеграції запропонованих моделей у прикладні системи та оцінка їх впливу на продуктивність і безпеку в реальних умовах.

4) Запропонована апроксимація ненормальних розподілів нормальним за допомогою мінімізації відстані Колмогорова-Смірнова є цікавим підходом, але його обґрунтування є дещо стислим. Варто було б більш детально пояснити, чому саме цей метод є прийнятним і які можуть бути його обмеження.

5) Результати моделювання атак вкладення та декодування представлені лише для обмеженого набору параметрів (розмірності n та дисперсії σ). Для більшої переконливості варто було б навести результати для ширшого діапазону параметрів та, можливо, для різних значень модуля q.

Чевардін В. Є.

1) У роботі дуальні атаки згадані лише побіжно. Відсутній їхній детальний математичний аналіз, кількісні оцінки складності та порівняння з атаками вкладення чи декодування; не розглянуто також вибір параметрів, що мінімізують ризик саме дуальних методів. Через це лишається неясним, наскількизапропоновані рекомендації забезпечують стійкість проти найсучасніших дуальних підходів до

криптоаналізу схем на решітках.
2) Оцінки стійкості подані розрізнено: параметри та результати для DSTU 8961/CRYSTALS-Kyber наведені в розділі 4, тоді як для Falcon і CRYSTALS-Dilithium — у розділі 5. Проте зведеної порівняльної таблиці, яка б концентровано демонструвала всі отримані оцінки (рівні безпеки, час атак, параметри редукції тощо) для всіх розглянутих схем, у роботі немає; це ускладнює швидке співставлення результатів і формування практичних рекомендацій.
3) У таблиці 1.1 наведено оцінки часу роботи алгоритмів просіювання на класичному комп'ютері, однак не вказано, яка з них є теоретичною оцінкою, а яка -експериментальною (практичною), отриманою на основі емпіричних досліджень. Відсутність такого розмежування ускладнює аналіз точності оцінок і їх прикладну інтерпретацію, особливо з урахуванням того, що значення констант та доданків виду o(β) можуть суттєво впливати на реальну складність атаки.
4) У джерелі [47], на яке посилається автор, важливу роль відіграє метод Карацуби, який використовується як один з основних способів оптимізації реалізації криптосистеми NTRU Prime. Однак у дисертації не розглянуто це питання, не надано аналізу або згадки про вибір методу множення поліномів. Урахування цих аспектів могло б підсилити практичну цінність роботи, а також дати ширше уявлення про ефективність реалізації.
Корченко О.Г.
1) Оцінка атак на Falcon, що використовують похибки з плаваючою точкою, не зіставлена з контр-заходами. В роботі докладно змодельовано атаку, та не подано цифр, які показали б, наскільки відомі методи захисту зменшують успішність зламу.
2) Експериментальна перевірка точності моделей редукції ґрунтується на решітках розмірності до 256, тоді як сучасні стандарти (Kyber, Dilithium, Falcon) працюють з більшими розмірностями; екстраполяція результатів на великі розмірності потребує окремого обґрунтування.
3) Оцінювання впливу квантових комп'ютерів для прискорення класичних атак в роботі зводиться до застосування консервативних моделей безпеки. Сучасні моделі, що враховують квантові гейти та особливості їх реалізації для квантових атак, в роботі не розглядаються, що зменшує практичну цінність отриманих оцінок.
4) В роботі проаналізована атака на реалізацію Falcon, проте для інших криптографічних перетворень така атака не розглядається.

Результати відкритого голосування:

«За» ___5____ членів ради,

«Проти» _____ членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує/ відмовляє у присудженні

__Кандію Сергію Олеговичу_____

(власне ім'я, прізвище, здобувача (ки) у давальному відмінку)

ступінь/ступеня доктора філософії з галузі знань __12 Інформаційні технології

(галузь знань)

за спеціальністю (спеціальностями) __**125 Кібербезпека**_____

(код і найменування спеціальності (спеціальностей)

_____.

відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Відеозапис трансляції захисту дисертації додається.

Окрема думка члена разової ради додається (за наявності).

Голова разової спеціалізованої вченої ради _____ Віталій ЄСІН_____

(підпис) (власне ім'я та прізвище)

М.П.