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

Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач (ка) ступеня доктора філософії _Каптьол Євгеній Юрійович_____,
(власне ім'я, прізвище здобувача (ки))
_1997__ року народження, громадянин (ка) _____України_____,
(назва держави, громадянином якої є здобувач (ка))
освіта вища: закінчив (ла) у _2019___ році Харківський національний університет імені В. Н. Каразіна _____
(найменування закладу вищої освіти)
за спеціальністю (спеціальностями) Кібербезпека _____,
(за дипломом)
працює аналітиком із систем захисту інформації в ПрАТ «ІІТ», _____
виконав (ла) акредитовану освітньо-наукову програму **Кібербезпека**.
Разова спеціалізована вчена рада, утворена наказом Харківського національного університету імені В.Н. Каразіна Міністерством освіти та науки України, м. Харків_____
(повне найменування закладу вищої освіти
_____ 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 Навчально-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)
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 «30» травня 2025 року прийняла рішення про присудження ступеня доктора

філософії з галузі знань 12 Інформаційні технології
(галузь знань)

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

на підставі публічного захисту дисертації «Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу»
(назва дисертації)

за спеціальністю (спеціальностями) 125 Кібербезпека.
(код і найменування спеціальності (спеціальностей)

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

Дисертацію виконано у (в) Харківському національному 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 Навчально-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 11 наукових публікацій за темою дисертації, з них 6 (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. Potii, O., Kachko, O., Kandii, S., & Kaptol, Y. (2024). Determining the effect of a floating point on the Falcon digital signature algorithm security. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 52–59. (Scopus, Web of Science) https://journals.uran.ua/eejet/article/view/295160/291714. DOI: 10.15587/1729-4061.2024.295160.
2. Kachko, O., Gorbenko, Y., Kandii, S., & Kaptol, Y. (2024). Improving protection of falcon electronic signature software implementations against attacks based on floating point noise. Eastern-European Journal of Enterprise Technologies, 4(9 (130), 6–17. (Scopus, Web of Science) https://journals.uran.ua/eejet/article/view/310521. DOI: 10.15587/1729-4061.2024.310521.
3. Kaptiol, Y. Y. (2022). Analysis of the RAINBOW post-quantum electronic signature algorithm state and attacks on it for the period of the NIST PQC third round completion. Radiotekhnika, 2(209), 87–92. http://rt.nure.ua/article/view/262495/258911. DOI: 10.30837/rt.2022.2.209.09.
4. Yu.I. Gorbenko, M.V. Yesina, V.A. Ponomar, I.D. Gorbenko, E.Yu. Kapt'ol Scientific and methodological bases of analysis, evaluation and results of comparison of existing and promising (post-quantum) asymmetric cryptographic primitives of electronic signature, protocols of asymmetric encryption and key encapsulation protocols. Radiotekhnika. 2023. 212, 42-66. http://rt.nure.ua/article/view/286512/280398. DOI: 10.30837/rt.2023.1.212.05.
5. Є. Ю. Каптьол, І. Д. Горбенко. Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері. Radiotekhnika, 202, 37-48. http://rt.nure.ua/article/view/215822/215989. DOI: 10.30837/rt.2020.3.202.03.
6. Gorbenko, I., & Kaptol, Y. (2023). Analysis and comparison of the security of electronic signatures based on new quantum-resistant problems. Radiotekhnika, 4(215), 31–45. http://rt.nure.ua/article/view/299724/292240. DOI: 10.30837/rt.2023.4.215.04.

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

Олійников Р. В.:

1) Розглянуто не всі види актуальних підходів до реалізації квантовостійких асиметричних електронних цифрових підписів. Так, серед кандидатів на додаткову стандартизацію наявні підписи засновані на кодах, підписи на ізогеніях, багатовимірні підписи, симетричні підписи, MPC-in-the-head та інші підписи, визначені NIST. Автор явно зосередився на тих кандидатах, які не потрапили в стандартну класифікацію та були виділені в «інші».

2) Оцінка та порівняльний аналіз в модифікації комплексної методики оцінки та порівняльного аналізу здійснено з урахуванням практичних застосувань ЕП, але не враховано частину поширених застосувань, таких як технології Blockchain, підписання коду, електронна пошта, електронні паспорти та загальна модель інфраструктури відкритих ключів (ІВК), хоча і були розглянуті окремі підпорядковані приклади ІВК.

3) У роботі зазначаються вимоги до квантовостійких криптографічних перетворень електронного підпису, які впливають на формування критеріїв оцінки та порівняльного аналізу, проте прямих порівнянь вимог не наведено, та процес формування критеріїв розглянуто частково, хоча в роботі все ж таки наявне посилання на відповідну статтю автора.

Толюпа С. В.:

1) Види актуальних підходів до реалізації квантовостійких асиметричних ЕП розглянуто частково. Серед кандидатів на додаткову стандартизацію ЕП автор явно зосередився на тих кандидатах, котрі не влучали в стандартну класифікацію та були виділені в «інші», та не приділив достатньої уваги тим, котрі підпадіють під категорії: підписи засновані на кодах, підписи на ізогеніях, мультиваріативні підписи, симетричні підписи, MPC-in-the-head.

2) З точки зору статистики та методів експертної оцінки, для отримання точних результатів необхідні значні обсяги вибірки. В дисертаційній роботі обсяги вибірки є відносно невеликими, хоча цей недолік частково усувається завдяки високій кваліфікації експертів та різноманітності їх підходів. Цей недолік признано автором та надано рекомендації щодо коректного застосування комплексної методики оцінки та порівняння.

3) В роботі відображено виявлену в процесі оцінки Falcon атаку на реалізацію та запропоновано рекомендації з підвищення безпеки та усунення загрози реалізації атаки. Проте не було відображено порівняння безпеки Falcon до застосування та після застосування пропозицій з підвищення безпеки з точки зору комплексної методики.

4) Деякі практичні застосування електронних підписів (наприклад, ІВК, SSL/TLS, DNSSEC, S/MIME, IPsec) розглядаються досить детально, з описом протоколів та алгоритмів. Інші ж застосування (підпис коду, SIM-карти, електронні паспорти, підписання PDF, технології Blockchain, VPN) згадуються більш поверхово, без глибокого аналізу їхніх специфічних вимог до електронних підписів. Це створює нерівномірне розуміння контексту.

5) В підрозділі 3.2. перелік безумовних критеріїв, наведений для протоколів інкапсуляції ключів (ПІК), містить критерії, які більше характерні для електронних підписів (ЦЕП, НЕП). Потрібно обґрунтувати включення цих критеріїв до оцінки ПІК або уточнити їхню інтерпретацію в цьому контексті.

Чевардін В. Є.:

1) У роботі було розглянуто в процесі оцінки та порівняння актуальні підходи до реалізації квантовостійких асиметричних ЕП, проте значна їх частина залишилась поза фокусом оцінки та порівняння. Так, наприклад, серед кандидатів на додаткову стандартизацію ЕП не були розглянуті підписи засновані на кодах, мультиваріативні підписи, симетричні підписи, тощо. Хоча комплексна методика і передбачає можливість її застосування до будь-якої множини ЕП, демонстрація застосування її до ширшого кола кандидатів на квантову стійкість посилила б обґрунтованість отриманих результатів.

2) У роботі зазначаються вимоги до квантовостійких криптографічних перетворень електронного підпису як на національному, так і на міжнародному рівнях. Ці вимоги є витоками критеріїв оцінки та порівняльного аналізу, проте в роботі питання процесу формування критеріїв з вимог знайшло лише часткове відображення.

3) У формулі 5.1 застосовується ділення на 10 як базис нормалізації зважених оцінок, проте в роботі не пояснюється, чому обрано саме це значення.
4) У роботі приділено увагу конкурсу NIST PQC, зокрема описано криптоаналітичні атаки на алгоритм Rainbow. Водночас інші кандидати, які були відхилені за результатами третього раунду (зокрема, GeMSS і Picnic), не згадані, хоча вони також належать до класу квантовостійких електронних підписів. Згадка про них могла б надати більш повну картину процесу оцінювання та відбору кандидатів і висвітлити обмеження окремих криптографічних підходів.

Корченко О. Г.:
1) Проведені оцінка та порівняльний аналіз в модифікації комплексної методики оцінки та порівняльного аналізу здійснені лише для таких засобів як: SSL/TLS, SIM-карти, IPSec, DNSSEC, VPN та підписання PDF, а порівняння для решт, таких як технології Blockchain, підписання коду, електронна пошта, електронні паспорти не були розглянуті. Автор обґрунтовує це подібністю цих застосувань до вже обраних та меншою їх релевантністю для прийняття оцінюваних алгоритмів за стандарт, проте це б забезпечило більшу повноту аналізу засобів пов'язаних з предметом дослідження.
2) У дисертаційній роботі висувається пропозиція з використання фіксованої точки замість плаваючої в процесі формування електронного підпису Falcon. Доцільно здійснити порівняння безпеки Falcon до та після застосування пропозицій з усунення загрози реалізації атаки та інших варіантів усунення такої загрози реалізації.
3) Наведені в дисертаційній роботі оцінки та порівняння мають обмежений обсяг вибірки, що призводить до зниження неупередженості отриманої оцінки.
4) В роботі використовується підхід до оцінювання та порівняльного аналізу на основі експертних методів, проте інші методи проведення оцінювання та порівняльного аналізу не розглянуто.

Результати відкритого голосування:

«За» ___5____ членів ради,

«Проти» ___0____ членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує

_Каптьолу Євгенію Юрійовичу_____

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

ступінь 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)

МП.