

## РІШЕННЯ

Вченої ради Харківського національного університету імені В. Н. Каразіна з питання: «Про утворення в Харківському національному університеті імені В. Н. Каразіна разової спеціалізованої вченої ради з правом прийняття до розгляду та проведення разового захисту дисертації здобувача Кандія Сергія Олеговича на тему «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак» на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації»  
**від 01 квітня 2025 року, протокол № 10**

Заслухавши та обговоривши інформацію проректора з науково-педагогічної роботи Олександра ГОЛОВКА, відповідно до пунктів 3, 17–18 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, та підпункту 26 п.13.2. Статуту Харківського національного університету імені В. Н. Каразіна Вчена рада ухвалила:

1. Утворити разову спеціалізовану вчену раду Харківського національного університету імені В.Н. Каразіна з правом прийняття до розгляду та проведення разового захисту дисертації здобувача Кандія Сергія Олеговича з метою присудження йому ступеня доктора філософії зі спеціальності 125 Кібербезпека та захист інформації у галузі знань 12 Інформаційні технології (додаток 1).

*Відповідальний: проректор з науково-педагогічної роботи Олександр ГОЛОВКО.*

Заступник голови Вченої ради



Учений секретар

Антон ПАНТЕЛЕЙМОНОВ

Олена ФРІДМАН

## Склад

разової спеціалізованої вченої ради з правом прийняття до розгляду та проведення разового захисту дисертації здобувача Кандія Сергія Олеговича на тему «Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак» на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації

Голова	Єсін Віталій Іванович	<p>Професор кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту у Харківського національного університету імені В. Н. Каразіна, доктор технічних наук, професор</p> <p>1. Yesin V.I., Vilihura V.V. Researching basic searchable encryption schemes in databases that support SQL. <i>Radiotekhnika</i>. 2022. Vol. 210. P. 53-74.</p> <p>2. Yesin V.I. Vilihura V.V. Research on the main methods and schemes of encryption with search capability. <i>Radiotekhnika</i>. 2022. Vol. 209. P. 138-155.</p> <p>3. Yesin V.I., Vilihura V.V., Svatowsky I.I. Ensuring security in distributed information systems: major aspects. <i>Radiotekhnika</i>. 2023. Vol. 214. P. 32-63.</p>
Рецензент	Олійников Роман Васильович	<p>Професор кафедри кібербезпеки інформаційних систем, мереж і технологій Навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна, доктор технічних наук, професор</p> <p>1. Rodinko M., Oliynykov R., Yubuzova K. Differential cryptanalysis of the lightweight block cipher Cypress-256. <i>International Journal of Computing</i>. 2020. 19(2). P. 273-281.</p> <p>2. Oliynykov R., Zhang J., Zhang B., Nastenka A., Balogun H. Privacy-Preserving Decision-Making Over Blockchain. <i>IEEE Transactions on Dependable and Secure Computing</i>. 2023. Vol. 20. №6. P. 4648-4663.</p> <p>3. Bepalov Y., Kovalchuk L., Nelasa H., Oliynykov R., Viglione R. Models for Generation of Proof Forest in zk-SNARK Based Sidechains. <i>Cryptography</i>. 2023. 7(1). Article number 14.</p>
Офіційний опонент	Толюпа Сергій Васильович	<p>Професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, доктор технічних наук, професор</p> <p>1. Толюпа С., Лаптев С. Удосконалення математичної моделі захищеності особистих даних за рахунок врахування довіри та кількості інформації в соціальних мережах. <i>Безпека інформації</i>. 2022. Vol. 28. P. 143-148.</p> <p>2. Толюпа С., Самохвалов Ю., Хусаїнов П., Штаненко С. Самодіагностування як спосіб підвищення кіберстійкості термінальних компонентів технологічної системи. <i>Кібербезпека: освіта, наука, техніка</i>. 2023. Vol 2. P. 135-</p>

		<p>147.</p> <p>3. Толюпа С., Шевченко А., Кулько А. Особливості забезпечення безпеки критичних інфраструктур. <i>Безпека інформаційних систем і технологій</i>. 2024. Vol 1. P. 11-23.</p>
Офіційний опонент	Чевардін Владислав Євгенійович	<p>Начальник кафедри кібербезпеки військового інституту телекомунікацій та інформатизації імені Героїв Крут, доктор технічних наук, старший науковий співробітник</p> <p>1. Stoikova, L.S., Chevardin, V.E. Exact Estimates of the Probability of a Random Variable Falling Into a Specified Interval in One Class of Unimodal Distributions. <i>Cybernetics and Systems Analysis</i>. 2023. Vol. 59. P. 986-996.</p> <p>2. Чевардін В.Є., Прийма О. О., Лаврик І.В. Криптосистеми на основі ізоморфних перетворень еліптичних кривих. <i>Системи і технології зв'язку, інформатизації та кібербезпеки</i>. 2024. Вип. №5(5). С. 230-241.</p> <p>3. Чевардін В.Є., Організаційно-технічні рішення щодо побудови захищених інформаційно-комунікаційних систем. <i>Системи і технології зв'язку, інформатизації та кібербезпеки</i>. 2024. Вип. №6. С. 250-263.</p>
Офіційний опонент	Корченко Олександр Григорович	<p>Професор кафедри безпеки інформаційних технологій національного авіаційного університету, доктор технічних наук, професор</p> <p>1. Shula V., Korchenko O., Zaritskyi O., Lozova I., Pedchenko Y. A multiple-theoretical GDPR model of parameters for personal data. <i>Ukrainian Information Security Research Journal</i>. 2023. Vol. 25. P. 254-268.</p> <p>2. Корченко О., Грищук О. Метод криптографічного захисту мовної інформації на основі диференціальних перетворень. <i>Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем</i>. 2024. Т.1. № 27. С. 4-19.</p> <p>3. Korchenko O., Ivanchenko E. Assessment system for enhancing cybersecurity posture of critical infrastructure inspection objects of the state. <i>Ukrainian Information Security Research Journal</i>. 2024. Vol. 30. P. 95-99.</p>