

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**  
**ІМЕНІ ТАРАСА ШЕВЧЕНКА**

«ЗАТВЕРДЖУЮ»

Ректор

\_\_\_\_\_ Володимир БУГРОВ  
« \_\_\_\_ » \_\_\_\_\_ 202\_ р.

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА**  
**«ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ КІБЕРЗАХИСТУ»**

**Рівень вищої освіти: перший**

**на здобуття освітнього ступеня: бакалавр**  
**за спеціальністю F5 «Кібербезпека та захист інформації»**  
**галузі знань F «Інформаційні технології»**

Розглянуто та затверджено  
на засіданні Вченої ради  
від « \_\_\_\_ » \_\_\_\_\_ 202\_ р.  
протокол № \_\_\_\_

Введено в дію наказом ректора  
від « \_\_\_\_ » \_\_\_\_\_ 202\_ за № \_\_\_\_

Київ 202\_ р.

**ЛИСТ ПОГОДЖЕННЯ**  
**освітньо-професійної програми**  
**«Інтелектуальні технології кіберзахисту»**

**1.1 Науково-методична рада:** протокол № \_\_\_\_\_ від «\_\_» \_\_\_\_\_ 20\_\_ р.

(особливі умови, за наявності)

Голова науково-методичної ради \_\_\_\_\_

**2.1 Планово-фінансовий відділ:**

(висновок, особливі умови, за наявності)

Начальник відділу \_\_\_\_\_ Ірина Дьолог «\_\_» \_\_\_\_\_ 20\_\_ р.

**2.2 Навчально-методичний відділ:**

(особливі умови, за наявності)

Директор НМВ \_\_\_\_\_ Андрій ПИЖИК «\_\_» \_\_\_\_\_ 20\_\_ р.

**2.3 Відділ забезпечення якості освіти:**

(особливі умови, за наявності)

Керівник ВЗЯО \_\_\_\_\_ Дарія ЩЕГЛЮК «\_\_» \_\_\_\_\_ 20\_\_ р.

**4.1 Вчена рада факультету комп'ютерних наук та кібернетики**

Протокол № \_\_\_\_\_ від «\_\_» \_\_\_\_\_ 20\_\_ р.

(особливі умови, за наявності)

Голова Вченої ради \_\_\_\_\_ Олена КАШПУР

**4.2 Науково-методична комісія факультету комп'ютерних наук та кібернетики**

Протокол № \_\_\_\_\_ від «\_\_» \_\_\_\_\_ 20\_\_ р.

(особливі умови, за наявності)

Голова науково-методичної комісії \_\_\_\_\_ Тетяна КАРНАУХ

**Розробники:**

1. Керівник проєктної групи Олена КАШПУР

Декан факультету комп'ютерних наук та кібернетики, професор кафедри обчислювальної математики,

д.ф.-м.н., доцент \_\_\_\_\_ «\_\_» \_\_\_\_\_ 2025 р.

**Члени проєктної групи:**

2. Ігор ЗАВАДСЬКИЙ

Професор кафедри математичної інформатики кібернетики факультету комп'ютерних наук та кібернетики,

д.ф.-м.н., професор \_\_\_\_\_ «\_\_»\_\_\_\_\_ 2025 р.

3. Людмила КОВАЛЬЧУК

провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова  
Національної академії наук України,

д.т.н., професор \_\_\_\_\_ «\_\_»\_\_\_\_\_ 2025 р.

4. Антон КУДІН

Головний експерт управління безпеки інформації Департаменту безпеки Національного банку  
України, член-кореспондент НАН України, лауреат державної премії України в галузі науки і  
техніки

д.т.н., старший науковий співробітник \_\_\_\_\_ «\_\_»\_\_\_\_\_ 2025 р.

5. Тарас ПАНЧЕНКО

Завідувач кафедри теорії та технології програмування факультету комп'ютерних наук та  
кібернетики,

к.ф.-м.н., доцент \_\_\_\_\_ «\_\_»\_\_\_\_\_ 2025 р.

6. Тетяна КАРНАУХ

Доцент кафедри теоретичної кібернетики факультету комп'ютерних наук та кібернетики,

к.ф.-м.н., доцент \_\_\_\_\_ «\_\_»\_\_\_\_\_ 2025 р.

7. Ольга СУПРУН

Доцент кафедри теорії та технології програмування факультету комп'ютерних наук та  
кібернетики,

к.ф.-м.н., доцент \_\_\_\_\_ «\_\_»\_\_\_\_\_ 2025 р.

8. Андрій ФІСУНЕНКО

Директор ТОВ «САМСУНГ РнД ІНСТИТУТ Україна»,

к.ф.-м.н., доцент \_\_\_\_\_ «\_\_»\_\_\_\_\_ 2025 р.

## **ІНФОРМАЦІЯ ПРО ВНУТРІШНЮ ТА ЗОВНІШНЮ АПРОБАЦІЮ**

А. Відгуки кафедр / загальноуніверситетських підрозділів.

Б. Рецензії представників академічної спільноти.

В. Відгуки представників професійних асоціацій.

Г. Відгуки представників ринку праці.

## ПЕРЕДМОВА

Розроблено робочою групою у складі:

Прізвище, ім'я, по батькові керівника та членів проектної групи	Найменування посади (для сумісників — місце основної роботи, найменування посади)	Найменування закладу, який закінчив викладач (рік закінчення, спеціальність, кваліфікація згідно з документом про вищу освіту)	Науковий ступінь, шифр і найменування наукової спеціальності, тема дисертації, вчене звання, за якою кафедрою (спеціальністю) присвоєно	Стаж науково-педагогічної та/або наукової роботи	Інформація про наукову та/або професійну діяльність, яка відповідає предметній області програми (основні публікації за напрямом, науково-дослідна робота, участь у конференціях і семінарах, робота з аспірантами та докторантами, керівництво науковою роботою студентів)	Відомості про підвищення кваліфікації викладача (найменування закладу, вид документа, тема, дата видачі)
<b>Керівник проектної групи</b>						

<p style="text-align: center;"><b>КАШПУР</b> <b>Олена Федорівна</b></p>	<p style="text-align: center;">Декан факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка</p>	<p style="text-align: center;">Київський державний університет імені Т. Шевченка (1992, прикладна математика, математик)</p>	<p style="text-align: center;">Доктор фізико-математичних наук, 01.05.02 - Математичне модельовання та обчислювальні методи» (ДД №013147, 22.10.2023 р.), «Інтерполяція операторів в гільбертових та евклідових просторах», доцент кафедри методів обчислювального експерименту (02ДЦ № 011439, 06.02.2006 р.)</p>	<p style="text-align: center;">28 років</p>	<p>Виконавиця міжнародного грантового проекту “Cybersecurity Seminar Program” у партнерстві з Google.org та Virtual Routes. Бере участь у міжнародних конференціях. Керує аспірантами, виконанням кваліфікаційних робіт бакалаврів і магістрів, курсових робіт здобувачів освіти. Основні публікації: 1.Makarov V. L., Khlobystov V. V., Kashpur O.F. Operator Interpolation and Systems of Linear Equations and Inequalities in Euclidean Spaces // Ukrainian Mathematical Journal. - april, 2021. - Vol. 72. - № 11. P. 1758 - 1770. 2.Kashpur O.F. Hermite–Birkhoff Interpolation Polynomial of Minimum Norm in Hilbert Space // Cybernetics and Systems Analysis. - 2021. - Vol. 57, Iss. 5. P. 803 -- 808. 3. Kashpur O., Boichenko B., Boychuk A. Fast Polynomial Reconstruction, PDMU-2025, XL International Conference ROBLEMS OF DECISION MAKING UNDER UNCERTAINTIES. 4. Kashpur O. F. Hermite Interpolation Polynomial for Functions of Several Variabl // Cybernetics and Systems Analysis. - 2022. - Vol. 58, Iss. 3. P. 399 - 408. 5. Kashpur O. F. Solving Hermite interpolation problem in finite- dimensional Euclidean space // Cybernetics and Systems Analysis. - 2022. - Vol. 58, Iss. 2. P. 259 –267. 6. Кашпур О. Ф. Фундаментальні поліноми інтерполяційної формули Ерміта в лінійному нормованому та в евклідових просторах // Журнал обчислювальної та прикладної</p>	<p>Київський національний університет імені Тараса Шевченка, 23.11- 01.12.2020, «Роль гарантів освітніх програм у розбудові внутрішньо системи забезпечення якості освіти», № 744-20. Київський національний університет імені Тараса Шевченка, 21-22.10.21, «Розбудова внутрішніх систем забезпечення якості освіти у ЗВО Україні», Сертифікат. Київський національний університет імені Тараса Шевченка, 11.05- 27.12.2022, «Роль гарантів освітніх програм у розбудові внутрішньо системи забезпечення якості освіти», № 627-22. Київський національний університет імені Тараса Шевченка, 10.01- 22.01.2024, «Етико-психологічне забезпечення реалізації куратором ЗВО завдань професійної соціалізації та патріотичного виховання студентів», KU 02070944/000062-24. Львівська політехніка, 13.03.2024, «Вивчення Європейського досвіду впровадження систем управління якістю освітніх послуг» в рамках міжнародного проекту Erasmus+Jean Monnet Module 101085516-QMSEEI – ERASMUS-JMO – 2022 HEI – TCH- RSCH. Київський національний університет імені Тараса Шевченка, 25-27.11.2024, «Практика підтримки ментального здоров'я», KU 02070944/001663-24. Київський національний університет імені Тараса Шевченка, 10-12.2024, «Стрес-менеджмент та техніки психологічної самопідготовки», KU 02070944/0011987-24.</p>
---	--	--	--	---	--	--

					<p>математики. - 2022. - № 2. С. 50 - 58.</p> <p>7. Makarov V. L., Sergienko I. V., Khimich O. M., Lyashko S. I., Samoilenko V. H., Kashpur O. F., Alexandrovich I. M., Klyushin D. A., Semenov V. V., Mayko N. V. Generalized analytic functions and summary representation method and their applications. In commemoration of the 110th anniversary of HM Polozhii's birth // Journal of Applied Mathematics. - 2024. - №2. - P. 66-76.</p> <p>8. Макаров В. Л., Кашпур О. Ф. Огляд теорії поліноміальної інтерполяції // Український математичний журнал - 2025., т. 77 - №7. С. 461 – 488.</p>	<p>CERTIFICATE, The University of L'Aquila (International Credit Mobility), 15.02.2025.</p>
--	--	--	--	--	--	---

Члени проектної групи						
<b>ЗАВАДСЬКИЙ Ігор Олександрович</b>	Професор кафедри математичної інформатики Київського національного університету імені Тараса Шевченка	Київський національний університет імені Тараса Шевченка (1996, прикладна математика, математик)	Доктор фізико-математичних наук, 01.05.01 – Теоретичні основи інформатики та кібернетики, (ДД № 010098 від 24.09.2020), «Подільні коди та їх застосування», професор кафедри математичної інформатики	25 років	<p>Автор більше 130 наукових та навчально-методичних праць; 20 підручників та посібників з грифом «Рекомендовано МОН України», навчальних програм з інформатики та освітніх стандартів, зокрема</p> <p>1. Zavadskyi I.O., Lossless text compression by means of binary-coded ternary number representation. <a href="#">Discrete Applied Mathematics</a>, vol. 354, p. 15–22, 2024.</p> <p>2. Zavadskyi, I., Kovalchuk, M. Binary Mixed-Digit Data Compression Codes. SPIRE. Lecture Notes in Computer Science, vol 14240, pp. 381–392, 2023.</p> <p>3. A.V. Anisimov, I.O. Zavadskyi. “Variable-Length Prefix Codes With Multiple Delimiters”, IEEE Transactions on Information Theory, Volume 63, Issue 5, pp. 2885–2895, 2017.</p>	<p>Курси підвищення кваліфікації «Information Security Risk Management Review course» в ISACA Kyiv Center, диплом від 25.11.2022.</p> <p>Стажування «Викладання фізико-математичних дисциплін із використанням цифрових інструментів», сертифікат № PhmSI-010402-KSW від 12.05.2024.</p>

<p><b>КОВАЛЬЧУК Людмила Василівна</b></p>	<p>Провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України</p>	<p>Київський державний університет ім. Т. Шевченка (1989 р., математика, математик-викладач)</p>	<p>Доктор технічних наук, 05.13.21 – Системи захисту інформації, (ДД № 007369, 28.04.2009р.), спецтема, професор кафедри інформаційних систем (АП № 000261, 12.12.2017р.)</p>	<p>34 роки</p>	<p>Автор понад 150 публікацій (з них 49 проіндексовані в наукометричній базі Scopus), 1 монографія, 7 навчальних посібників. 1. Kovalchuk L.V., Koriakov I.V., Alekseychuk A.N. Cybernetics and Systems Analysis, 2023, 59(1), pp. 16–26. DOI: <a href="https://www.scopus.com/record/display.uri?eid=2-s2.0-85148413086&amp;origin=resultslist">https://www.scopus.com/record/display.uri?eid=2-s2.0-85148413086&amp;origin=resultslist</a> 2. Kovalchuk, L., Rodinko, M., Oliynykov, R. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2023, 13619 LNCS, pp. 275–293. DOI: <a href="https://www.scopus.com/record/display.uri?eid=2-s2.0-85149863201&amp;origin=resultslist">https://www.scopus.com/record/display.uri?eid=2-s2.0-85149863201&amp;origin=resultslist</a> 3. Bessalov A.V., Kovalchuk, L., V., Abramov S.V. Randomization of csidh algorithm on quadratic and twisted edwards curves. Кібербезпека: освіта, наука, техніка, №17, 2022, С.128-144. <a href="https://doi.org/10.28925/2663-4023.2022.17.128144">https://doi.org/10.28925/2663-4023.2022.17.128144</a>. 4. Lyudmila Kovalchuk, Nataliia Kuchynska, Hanna Nelasa Comparison of efficiency of Double Spend Attack for blockchains with checkpoints and without them // Фізико-математичне моделювання та інформаційні технології, (№36), pp. 12-16. 5. Kovalchuk L., Kostanda V., Marukhnenko O., Kuchynska N., Marchuk Y. Mathematics, 2023, 11(19), 4158. DOI: <a href="https://www.scopus.com/record/display.uri?eid=2-s2.0-85176426066&amp;origin=resultslist">https://www.scopus.com/record/display.uri?eid=2-s2.0-85176426066&amp;origin=resultslist</a> Керівник докторантів (захисти відбулись у 2024 та 2017 роках) та аспірантів (захисти відбулись у 2014 та 2021 роках),</p>	<p>ISACA Kyiv Chapter, “Information security risk management review course”, 180 годин, 25.11.2022. Кібергігієна 2, 6 годин, ВІТІ ім. Героїв Крут, 24.05.23. Інститут післядипломної освіти НТУУ “КПІ ім. Ігоря Сікорського” Організація дистанційного навчання за допомогою Microsoft Teams, 108 годин, 15.05.2025.</p>
---	---	--	---	----------------	---	--

					кваліфікаційних та курсових робіт здобувачів освіти. Бере участь у міжнародних конференціях.	
--	--	--	--	--	---	--

<p style="text-align: center;"><b>КУДІН</b> <b>Антон Михайлович</b></p>	<p style="text-align: center;">Головний експерт управління безпеки інформації Департаменту безпеки Національного банку України, професор кафедри Математичних методів захисту інформації Фізико-технічного інституту НГУУ «КПІ імені Ігоря Сікорського»</p>	<p style="text-align: center;">Київське вище інженерне радіотехнічне училище ППО ім. маршала авіації Покришкіна О.І., (1993, математичне забезпечення автоматизованих систем управління, інженер-математик)</p>	<p style="text-align: center;">Доктор технічних наук, 05.13.21 – Системи захисту інформації (ДД № 003256, 3.04.2014), спецтема, старший науковий співробітник за спеціальністю озброєння і військова техніка (АС № 001984, 19.10.2001 р.)</p>	<p style="text-align: center;">32 роки</p>	<p>Керівник міжнародного грантового проекту (НГУУ «КПІ імені Ігоря Сікорського та USID) «Розподілена система раннього виявлення вторгнень та оцінки кібербезпеки» № договору: G -202102-67499 Дата реєстрації: 2021-07-19 Основні публікації: 1. Tkach, V.; Kudin, A.; Kebande, V.R.; Baranovskyi, O.; Kudin, I. Non-Pattern-Based Anomaly Detection in Time-Series / MDPI Electronics 2023,12,721. Категорія «А» ISSN 2079-9292 <a href="https://doi.org/10.3390/electronics12030721">https://doi.org/10.3390/electronics12030721</a> 2. V. Tkach, A. Kudin, V. Zadiraka, I. Shvidchenko Signatureless anomalous behavior detection in information systems / Кібернетика та системний аналіз. – 2023. – Том.59. - № 5. – С.100-112. Категорія «А» ISSN 1019-5262 (Kibernetika ta Systemnyi Analiz, Print) ISSN 2522-9664 (Kibernetika ta Systemnyi Analiz, Online) <a href="https://doi.org/10.1007/s10559-023-00613-y">https://doi.org/10.1007/s10559-023-00613-y</a> 3. Кудін А.М., Кудін І.А., Чіхладзе В.З. Застосування загальної теорії оптимальних алгоритмів в криптографії, стеганографії та блокчейн-технології / Кібернетика та системний аналіз. – 2025. – Том.61. - № 4. – С.46-57. Категорія «А» ISSN 1019-5262 (Kibernetika ta Systemnyi Analiz, Online) <a href="https://doi.org/10.34229/kca2522-9664">https://doi.org/10.34229/kca2522-9664</a></p>	<p>Член-кореспондент Національної Академії Наук України за спеціальністю «Кібербезпека» (2024)</p>
---	---	---	---	--	--	--

<p><b>ПАНЧЕНКО Тарас Володимирович</b></p>	<p>Завідувач кафедри теорії та технології програмування Київського національного університету імені Тараса Шевченка</p>	<p>Київський національний університет імені Тараса Шевченка (2001, інформатика, магістр інформатики)</p>	<p>Кандидат фізико-математичних наук, 01.05.03 – Математичне та програмне забезпечення обчислювальних машин і систем (ДК №035862, 04.06.2006), «Композиційні методи специфікації та верифікації програмних систем», доцент кафедри теорії та технології програмування (12ДЦ №041378, 25.02.2015)</p>	<p>22 роки</p>	<p>Керівник міжнародного грантового проекту “Cybersecurity Seminar Program” у партнерстві з Google.org та Virtual Routes. Член європейських комітетів ACM, член правління ACM Ukraine, співзасновник ГО “Хакатон Експерт” Ментор, член журі ряду хакатонів, включно міжнародні: Bridging the Gap Hackathon, CSC Hackathon, FTI Hackathon Основні публікації: 1. T. Panchenko, A. Yavorskyi, M. Smilenko Effective Approaches for ECG Analysis: The 3rd International Scientific-Practical Conference «Development of modern science, experience and trends». – Boston, USA. – 2022. – P. 354-357. 2. T. Panchenko, V. Kubytskyi Enriched Image Embeddings as a Combined Outputs from Different Layers of CNN for Various Image Similarity Problems More Precise Solution: In: Hu, Z., Zhang, Q., He, M. (eds) Advances in Artificial Systems for Logistics Engineering III. The International Conference on Artificial Intelligence and Logistics Engineering (ICAILE 2023). Lecture Notes on Data Engineering and Communications Technologies. – Springer Nature Switzerland, Cham. – 2023. – Vol. 180. – pp. 321–333. 3. T. Panchenko, M. Kovalchuk, V. Kharchenko, A. Yavorskyi, I. Bieda Neural Networks-Based Method for Electrocardiogram Classification: International Journal of Computer Science and Network Security. 2023. Vol.23. No.9. P. 186–191.</p>	<p>Курс «DeepLearning.AI TensorFlow Developer», 20.06-20.08.2023 (90 годин/3 кредити ЄКТС). Сертифікат. SoftServe Academy course CLOUD ENVIRONMENT CONFIGURATION AND SECURITY, April 2024, Certificate Series BF № 17751/2024. Google Center of Excellence in Cybersecurity Google.org Cybersecurity Seminar Program Network Event in Malaga, Spain, 02-03.12.2024. Сертифікат від 06.01.2025</p>
--	---	--	--	----------------	---	---

<p><b>КАРНАУХ Тетяна Олександрівна</b></p>	<p>Доцент кафедри теоретичної кібернетики Київського національного університету імені Тараса Шевченка</p>	<p>Київський національний університет імені Тараса Шевченка (1997, прикладна математика, математик, викладач математики та інформатики (диплом з відзнакою АКІ № 97004301))</p>	<p>Кандидат фізико-математичних наук, 01.01.08 - Математична логіка, теорія алгоритмів і дискретна математика (ДК № 034851 від 08.06.2006 р.), “Класифікація функцій та чисел, що визначаються трансформаційними та генеруючими моделями обчислень”, доцент кафедри теоретичної кібернетики (12ДЦ № 022695 від 21.05.2009 р.)</p>	<p>24 роки</p>	<p>Автор 50 публікації, у тому числі 8 навчальних посібників (з яких 2 навчальні посібники з грифом МОН України), серед них серія посібників "Вступ до програмування мовою C++" (у співавторстві), посібник з грифом МОНУ "Комбінаторика". Проводить наукові дослідження в галузі теорії алгоритмів; вибрані наукові статті: "Дійсні числа та функції, обчислювані з поверненнями", "Метрично-можливий підхід до задач розпізнавання", "Qualitative estimation of plagiarism presence in programming assignment submissions". Бере участь у міжнародних конференціях, керівник дипломних та курсових робіт студентів.</p>	<p>Експерт з акредитації освітніх програм: онлайн тренінг та Як написати якісний звіт про результати акредитаційної експертизи освітньої програми (надані Національним агентством із забезпечення якості вищої освіти через платформу масових відкритих онлайн-курсів Prometheus, 2023, <a href="https://certs.prometheus.org.ua/cert/7379602b848d4fc6acfb6e817d1c7d76a">https://certs.prometheus.org.ua/cert/7379602b848d4fc6acfb6e817d1c7d76a</a>). SoftServe Academy course “Tech Summer Bootcamp for Teachers” (10 годин, 2023, Серія IA № 14501/2023). W3Cx Professional Certificate via edX “Front-End Web Developer” (2022, <a href="https://credentials.edx.org/credentials/689418ae3d5f4f3289b7e0470ab21cf6/">https://credentials.edx.org/credentials/689418ae3d5f4f3289b7e0470ab21cf6/</a>). Coursera certificate “Introduction to Software Testing” (30 годин, 2023, <a href="https://coursera.org/verify/4RE9ZYSMPHNB">https://coursera.org/verify/4RE9ZYSMPHNB</a>). Курс “ІТ-інструменти для викладачів” (GlobalLogic) (18 годин, липень 2023 р.). Coursera Professional Certificate “Google IT Automation with Python” (<a href="https://coursera.org/verify/professional-cert/VM7VFQW93EHW">coursera.org/verify/professional-cert/VM7VFQW93EHW</a>, 2020). Teacher’s Internship program held by EPAM Systems (Асоціація «Інформаційні технології України», січень 2019, сертифікат №0120). Етико-психологічне забезпечення реалізації куратором ЗВО завдань освітньо-професійної соціалізації та патріотичного виховання студентів (10-22 січня 2024 року, 1 кредит, КУ 02070944/000061-24) Психолого-педагогічний супровід</p>
--	---	---	---	----------------	---	---

						<p>психологічної компетентності спеціалістів ЗВО (10-31 травня 2023 року, 1 кредит, КУ 02070944/000839-23) SoftServe Academy “CLOUD ENVIRONMENT CONFIGURATION AND SECURITY” 15 лютого 2024 – 16 квітня 2024 XN № 17860/2024 , April 16, 2024, 4 кредити.</p>
--	--	--	--	--	--	--

<p style="text-align: center;"><b>СУПРУН Ольга Миколаївна</b></p>	<p>Доцент кафедри теорії та технології програмування Київського національного університету імені Тараса Шевченка</p>	<p>Київський державний університет ім. Т. Шевченка (1983, прикладна математика, математик)</p>	<p>Кандидат фізико-математичних наук, 01.01.06 - Алгебра і теорія чисел (КН № 008677, 18.08.1995), «Локально компактні групи з деякими обмеженнями для операцій перерізу та топологічного породження підгруп», доцент кафедри вищої математики (ДЦ АР№005514, 23.03.1997)</p>	<p>32 роки</p>	<p>Виконавця міжнародного грантового проєкту “Cybersecurity Seminar Program” у партнерстві з Google.org та Virtual Routes Основні публікації: 1. Фахівець сфери захисту інформації. Професійний стандарт. Головенко А., Бурбела О, Волкова К. та інші, всього 20 осіб. Затверджено Наказ Адміністрації Держспецв’язку 25 листопада 2022 року №715. С.39. 2. Фахівець з технічного захисту інформації. Професійний стандарт. Воронов В., Гайдур Г., Гулак Г. та інші, всього 21 особа. Затверджено Наказ Адміністрації Держспецв’язку 23 січня 2024 року №38. С.41. 3. Фахівець з криптографічного захисту інформації. Професійний стандарт. Воронов В., Гайдур Г., Гулак Г. та інші, всього 21 особа. Затверджено Наказ Адміністрації Держспецв’язку 23 січня 2024 року №38. С.28. 4. Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту. Професійний стандарт. Бабаніна В., Бакалинський О., Юдін О. та інші, всього 24 особи. Затверджено Наказ Адміністрації Держспецв’язку 23 січня 2024 року №38. С.28. 5. O.Suprun, O. Provotar, O. Suprun, O. Nechyporuk, V. Lukashenko, N. Zhuravel Development of a modified steganographic model of data transmission using IPv6 protocol: Proceedings of the Third International Conference on Cyber Hygiene &amp; Conflict Management in Global Information Networks (CH&amp;CMiGIN 2024), Kyiv, Ukraine, January 24–27, 2024. P. 35-46. <a href="https://ceur-ws.org/Vol-3925/paper04.pdf">https://ceur-ws.org/Vol-3925/paper04.pdf</a> Бере участь у міжнародних конференціях, керівник дипломних та курсових робіт</p>	<p>Курс аудиторів за стандартами серії ДСТУ ISO/IEC 27001 (40 годин). Сертифікат за кваліфікаційним рівнем: кандидат в аудитори (№ К 010, від 15 січня 2021 р). Курс «Оцінювач результатів навчання здобувачів професійної кваліфікації у сфері інформаційних технологій та кібербезпеки» у рамках реалізації Проєкту USAID «Кібербезпека критично важливої інфраструктури України». 20-25 червня 2022, 2 кредити ЄКТС Сертифікат. Навчання за програмою підвищення кваліфікації “Carpathian Winter Cybersecurity Week 2024”, 14-27.01.2024, 1 кредит ЄКТС (Свідоцтво № 23, 27.02.2024). International skill development (Webinar) on the topic “Funds Of Grant Activities And Fundraising: Foreign And National Experience”, 20-29.03.2024, Lublin (republic of Poland) (45 годин/1,5 кредитів ЄКТС). Сертифікат ES № 19188 від 29.03.2024. Google Center of Excellence in Cybersecurity Google.org Cybersecurity Seminar Program Network Event in Malaga, Spain, 02-03.12.2024, Сертифікат від 06.01.2025. Тренінг “Основи безпеки систем промислового управління, диспетчерського контролю та збору даних” на базі лабораторії кібербезпеки автоматизованих систем керування КПП ім. Ігоря Сікорського, січень 2025, 1 кредит ЄКТС (сертифікат 7ee684bb-1b41-</p>
---	--	--	---	----------------	---	--

					студентів.	4395-bd6a-e3ed783776ae).
<b>ФІСУНЕНКО</b> Андрій Леонідович	Директор ТОВ «САМСУНГ РІД ІНСТИТУТ УКРАЇНА»	Московський державний інженерно- фізичний інститут (технічний університет), (1994, теоретична ядерна фізика, інженер-фізик) Київський національний університет імені Тараса Шевченка, (2016, прикладна математика, математик)	Кандидат фізико-математичних наук, 01.05.01 - Теоретичні основи інформатики та кібернетики, «Побудова генератора геометричних об'єктів із заданими властивостями на площині»	31 рік	Автор 12 публікацій та тез конференцій, автор та співавтор 7 патентів з реєстрацією в усіх основних міжнародних юрисдикціях. 1. A. Fisunenko, Y. Yakishyn, M. Alieksieiev Deformable display device and image display method using same. US Patent 10,606,350, 2020. 2. A. Fisunenko, S. Pometun, O. Kulakov, A. Malyshev, O. Viatchaninov, V. Stupakov, V. Dziubliuk Apparatus and method for infinitely reproducing frames in electronic device. US Patent 11,048,959, 2021. З 2022 року відповідальний за напрям «Стратегія та інновації»: розробка і імплементації стратегії створення та функціонування R&D центру Samsung в Україні із спеціалізацією на технологіях кіберзахисту та ШІ. Організатор та виконавець 54 спільних дослідницьких проєктів з провідними університетами України у сферах кібербезпеки та штучного інтелекту, а також програм стажування і практик для студентів та аспірантів в Самсунг R&D у напрямах кібербезпеки, штучного інтелекту й технологій розширеної реальності, які охопили понад 400 стажерів-випускників.	Підвищення кваліфікації, НТУУ «Київський Політехнічний інсти- тут», Фізико-технічний інститут, Центр передпідготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки. Свідотво СПК АЕ №199629, напрям «Організація захисту мовної інформації у телекомунікаційних мережах і системах зв'язку».

При розробці проєкту Освітньої програми враховані вимоги:

- Стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації 12 Інформаційні технології для першого (бакалаврського) рівня вищої освіти, затверджений наказом Міністерства освіти і науки України від 29.10.2024 № 1547;
- Тимчасового стандарту вищої освіти першого рівня (ступінь бакалавра), галузь знань F Інформаційні технології за спеціальністю F5 Кібербезпека та захист інформації, затвердженого рішенням Вченої ради Університету від 27.01.2025 року, протокол №6;
- Постанови Кабінету Міністрів України від 19 травня 2021 р. № 497 «Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту».

**1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ**  
**«Інтелектуальні технології кіберзахисту» /**  
**«Intelligent Cybersecurity Technologies»**  
**зі спеціальності F5 «Кібербезпека та захист інформації»**

<b>1 – Загальна інформація</b>	
<b>Ступінь вищої освіти та назва кваліфікації</b>	Ступінь вищої освіти: Бакалавр Спеціальність: F5 Кібербезпека та захист інформації Кваліфікація: Бакалавр з кібербезпеки та захисту інформації / Higher Education Degree: Bachelor's Degree Specialty: F5 Cybersecurity and Information Protection Qualification: Bachelor in Cybersecurity and Information Protection
<b>Мови навчання і оцінювання</b>	Українська, англійська / Ukrainian, English
<b>Обсяг освітньої програми</b>	4 академічних роки, 240 кредитів ЄКТС / 4 academic years, 240 ECTS credits
<b>Тип програми</b>	Освітньо-професійна / Educational-Professional
<b>Тип диплома</b>	Диплом ЗВО / Diploma of Higher Education Institution
<b>Повна назва закладу вищої освіти, а також структурного підрозділу у якому здійснюється навчання</b>	Київський національний університет імені Тараса Шевченка, факультет комп'ютерних наук та кібернетики / Taras Shevchenko National University of Kyiv, Faculty of Computer Science and Cybernetics.
<b>Назва закладу вищої освіти який бере участь у забезпеченні програми</b>	–
<b>Офіційна назва освітньої програми, ступінь вищої освіти та назва кваліфікації ЗВО-партнера мовою оригіналу</b>	–
<b>Наявність акредитації</b>	–
<b>Цикл/рівень програми</b>	НРК України – 6 рівень, FQ-EHEA –перший цикл, EQF-LLL – 6 рівень
<b>Передумови</b>	Наявність атестату про повну загальну середню освіту
<b>Форма навчання</b>	Денна
<b>Термін дії освітньої програми</b>	5 років
<b>Інтернет-адреса постійного розміщення опису освітньої програми</b>	<a href="http://csc.knu.ua/uk/curriculum">http://csc.knu.ua/uk/curriculum</a>
<b>2 – Мета освітньої програми</b>	

<b>Мета програми (з урахуванням рівня кваліфікації)</b>	Підготовка фахівців, здатних розробляти та впроваджувати сучасні рішення у сфері кіберзахисту, а також створювати програмні продукти з використанням інтелектуальних технологій у сфері кібербезпеки та захисту інформації.
<b>3 - Характеристика освітньої програми</b>	
<b>Опис предметної області (галузь знань / спеціальність / спеціалізація програми)</b>	<p><b>Об'єкти вивчення:</b></p> <ul style="list-style-type: none"> <li>- технології кібербезпеки та захисту інформації;</li> <li>- процеси управління кібербезпекою та захистом інформації;</li> <li>- об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології.</li> </ul> <p><b>Цілі навчання:</b> підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації.</p> <p><b>Теоретичний зміст предметної області:</b> Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.</p> <p><b>Методи, методики та технології:</b> методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації.</p> <p><b>Інструменти та обладнання:</b> засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).</p>
<b>Орієнтація освітньої програми</b>	Освітньо-професійна академічна.
<b>Основний фокус освітньої програми та спеціалізації</b>	Загальна освіта за спеціальністю F5 «Кібербезпека та захист інформації». Ключові слова: кібербезпека; захист інформації; штучний інтелект у безпеці; криптологія; виявлення та протидія кіберзагрозам; аналіз вразливостей; управління інцидентами інформаційної безпеки.
<b>Особливості програми</b>	Освітній процес включає вивчення інтелектуальних технологій, зокрема методів

	штучного інтелекту, машинного навчання для виявлення та запобігання складним кіберзагрозам.
<b>4 – Придатність випускників до працевлаштування та подальшого навчання</b>	
<b>Придатність до працевлаштування</b>	На посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 «Кібербезпека та захист інформації».
<b>Подальше навчання</b>	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
<b>5 – Викладання та оцінювання</b>	
<b>Викладання та навчання</b>	Студентоцентроване навчання. Лекції, практичні заняття, семінарські заняття, курсова робота, лабораторні роботи, самостійна робота на основі навчально-методичних матеріалів, консультації з викладачами, виробнича практика, кваліфікаційна робота бакалавра, проектно-орієнтоване навчання.
<b>Оцінювання</b>	Письмові та усні іспити, звіти до лабораторних робіт, усні презентації, поточний контроль, заліки, диференційовані заліки, захист кваліфікаційної роботи бакалавра та єдиний державний кваліфікаційний іспит.

<b>6 – Програмні компетентності</b>	
<b>Інтегральна компетентність</b>	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
<b>Загальні компетентності (ЗК)</b>	<p><b>ЗК1.</b> Здатність застосовувати знання у практичних ситуаціях.</p> <p><b>ЗК2.</b> Знання та розуміння предметної області і розуміння професійної діяльності.</p> <p><b>ЗК3.</b> Здатність спілкуватися державною мовою як усно, так і письмово.</p> <p><b>ЗК4.</b> Здатність спілкуватися іноземною мовою.</p> <p><b>ЗК5.</b> Здатність вчитися і оволодівати сучасними знаннями.</p> <p><b>ЗК6.</b> Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.</p> <p><b>ЗК7.</b> Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.</p> <p><b>ЗК8.</b> Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p>

	<p><b>ЗК9*</b>. Здатність захищати Батьківщину.</p> <p><b>ЗК10</b>. Здатність до абстрактного мислення, аналізу та синтезу.</p> <p><b>ЗК11</b>. Здатність виявляти, ставити та вирішувати проблеми.</p> <p><b>ЗК12</b>. Цінування та повага різноманітності та мультикультурності.</p> <p><b>ЗК13</b>. Здатність виявляти ініціативу та підприємливість.</p> <p><b>ЗК14</b>. Прагнення до збереження навколишнього середовища.</p> <p><b>ЗК15</b>. Здатність діяти соціально відповідально та свідомо.</p>
<b>Спеціальні компетентності</b>	<p><b>СК1</b>. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.</p> <p><b>СК2</b>. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.</p> <p><b>СК3</b>. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.</p> <p><b>СК4</b>. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.</p> <p><b>СК5</b>. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.</p> <p><b>СК6</b>. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)</p> <p><b>СК7</b>. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.</p> <p><b>СК8</b>. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p> <p><b>СК9</b>. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p><b>СК10</b>. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.</p> <p><b>Додаткові фахові компетентності, пов'язані з особливостями освітньої програми:</b></p> <p><b>СК11</b>. Здатність використовувати методи штучного інтелекту, машинного навчання для виявлення, класифікації та прогнозування кіберзагроз.</p> <p><b>СК12</b>. Здатність оцінювати ефективність інтелектуальних технологій кіберзахисту, враховуючи їх вплив на безпеку, продуктивність і стійкість інформаційних систем.</p>
<b>7 – Програмні результати навчання</b>	
<b>Програмні результати навчання</b>	<p><b>ПРН1</b>. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.</p> <p><b>ПРН2</b>. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.</p> <p><b>ПРН3</b>. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.</p> <p><b>ПРН4</b>. Організувати власну професійну діяльність, обирати і</p>

	<p>використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.</p> <p><b>ПРН5.</b> Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.</p> <p><b>ПРН6.</b> Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.</p> <p><b>ПРН7.</b> Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.</p> <p><b>ПРН8.</b> Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обрати раціональний метод вирішення.</p> <p><b>ПРН9.</b> Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.</p> <p><b>ПРН10.</b> Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.</p> <p><b>ПРН11.</b> Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.</p> <p><b>ПРН12.</b> Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.</p> <p><b>ПРН13.</b> Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.</p> <p><b>ПРН14.</b> Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.</p> <p><b>ПРН15.</b> Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.</p> <p><b>ПРН16.</b> Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.</p> <p><b>ПРН17.</b> Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.</p>
--	---

	<p><b>ПРН18.</b> Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p> <p><b>ПРН19.</b> Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.</p> <p><b>ПРН20.</b> Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.</p> <p><b>ПРН21.</b> Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.</p> <p><b>ПРН22**.</b> Опанувати базові загальновійськові знання та вміння, необхідні для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України.</p> <p><b>Додаткові програмні результати навчання, пов'язані з особливостями освітньої програми:</b></p> <p><b>ПРН23.</b> Застосовувати методи машинного навчання, штучного інтелекту та нейронних мереж для побудови моделей виявлення, прогнозування та запобігання кіберзагрозам.</p> <p><b>ПРН24.</b> Виконувати впровадження інтелектуальних технологій в системи інформаційної безпеки організації та оцінювати їх.</p>
<b>8 – Ресурсне забезпечення реалізації програми</b>	
<b>Специфічні характеристики кадрового забезпечення</b>	До освітнього процесу долучені викладачі, що є професіоналами практиками галузі кібербезпеки та захисту інформації.
<b>Специфічні характеристики матеріально-технічного забезпечення</b>	Здобувачі освіти мають доступ до лабораторії штучного інтелекту, яка функціонує на факультеті комп'ютерних наук та кібернетики.
<b>Специфічні характеристики інформаційного та навчально-методичного забезпечення</b>	Використання електронної бібліотеки факультету комп'ютерних наук та кібернетики ( <a href="http://csc.knu.ua/uk/library">http://csc.knu.ua/uk/library</a> ) та авторських розробок науково-педагогічних працівників факультету.
<b>9 – Академічна мобільність</b>	
<b>Національна кредитна мобільність</b>	—
<b>Міжнародна кредитна мобільність</b>	—
<b>Навчання</b>	Навчання іноземних здобувачів здійснюється на загальних умовах.

<b>іноземних здобувачів вищої освіти</b>	
--	--

\*Обов'язкова для здобувачів освіти - громадян України, які навчаються за денною або дуальною формою здобуття освіти, і для яких, згідно із Законом України «Про військовий обов'язок і військову службу», проходження базової підготовки є обов'язковим.

\*\* Обов'язковий для здобувачів освіти - громадян України, які навчаються за денною або дуальною формою здобуття освіти, і для яких, згідно із Законом України «Про військовий обов'язок і військову службу», проходження базової підготовки є обов'язковим.

## 2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

### 2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
<b>Обов'язкові компоненти ОП</b>			
ОК.01	Вступ до університетських студій	2	Залік
ОК.02	Українська та зарубіжна культура	3	Залік
ОК.03	Філософія	4	Іспит
ОК.04	Соціально-політичні студії	2	Залік
ОК.05	Вибрані розділи трудового права і основ підприємницької діяльності	3	Залік
ОК.06	Іноземна мова	9	Залік
ОК.07	Іноземна мова для академічних цілей і за професійним спрямуванням	8	Іспит
ОК.08	Науковий образ світу	3	Залік
ОК.09	Екологічні й економічні процеси та їх моделювання	3	Залік
ОК.10	Дискретна математика	8	Іспит
ОК.11	Алгебра	7	Іспит
ОК.12	Математичний аналіз	10	Іспит
ОК.13	Програмування	10	Іспит
ОК.14	Фізичні основи захисту інформації	3	Залік
ОК.15	Вступ до спеціальності	3	Залік
ОК.16	Архітектура обчислювальних систем та комп'ютерні мережі	5	Залік
ОК.17	Розвиток комунікативних навичок та групова динаміка	3	Залік
ОК.18	Теорія ймовірностей та математична статистика	5	Іспит
ОК.19	Математичні основи криптології	7	Іспит
ОК.20	Алгоритми та структури даних	3	Іспит
ОК.21	Бази даних	4	Іспит
ОК.22	Основи мережевої безпеки	4	Залік
ОК.23	Основні положення інформаційної та кібернетичної безпеки	3	Залік
ОК.24	Теорія інформації та кодування	4	Залік
ОК.25	Системне програмування, операційні системи та їх безпека	8	Іспит
ОК.26	Криптографічний та стеганографічний захист інформації	4	Іспит
ОК.27	Нейронні мережі та основи штучного інтелекту	4	Іспит
ОК.28	Технічні засоби захисту інформації	4	Іспит
ОК.29	Низькорівневі вразливості програмного забезпечення	4	Залік

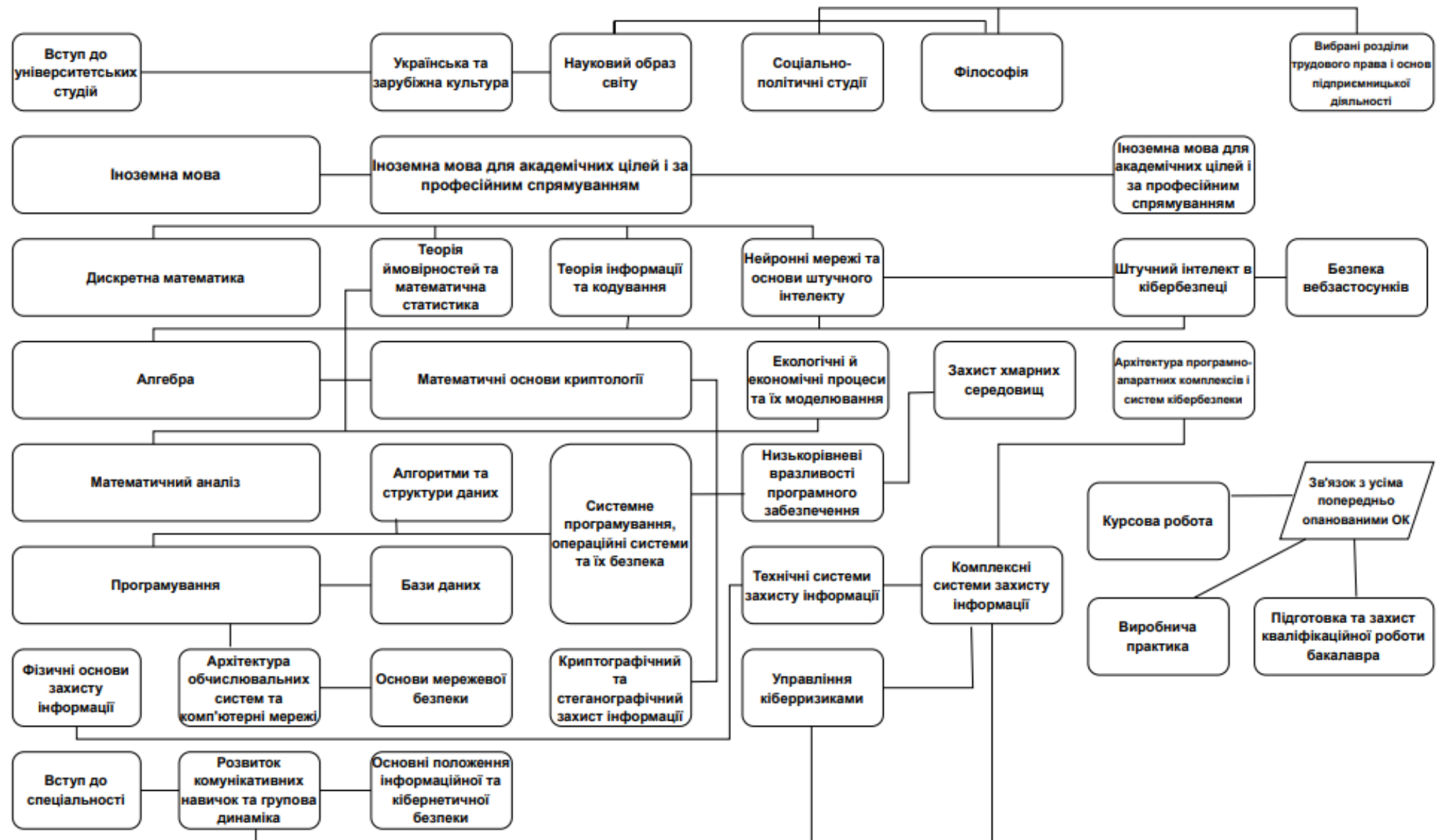
ОК.30	Управління кіберризиками	4	Іспит
ОК.31	Комплексні системи захисту інформації	4	Іспит
ОК.32	Захист хмарних середовищ	3	Іспит
ОК.33	Виробнича практика	6	Диф.залік
ОК.34	Курсова робота	2	Диф.залік
ОК.35	Штучний інтелект в кіберзахисті	3	Іспит
ОК.36	Архітектура програмно-апаратних комплексів і систем кібербезпеки	4	Іспит
ОК.37	Безпека вебзастосунків	3	Іспит
ОК.38	Підготовка та захист кваліфікаційної роботи бакалавра	8	Захист
<b>Загальний обсяг обов'язкових компонент:</b>		<b>177,0</b>	
<b>Вибіркові компоненти ОП*</b>			
ВК.01	Базова загальновійськова підготовка (теоретична частина)**	3	Диф.залік
<b>Загальний обсяг вибірових компонент:</b>		<b>63</b>	
<b>ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ</b>		<b>240</b>	

\* У межах обсягу вибіркової складової здобувач освіти має право обирати освітні компоненти самостійно, не обмежуючись пропозиціями навчального плану програми, на якій він навчається, згідно з п. 9.4 «Положення про організацію освітнього процесу в Київському національному університеті імені Тараса Шевченка» та п. 3.7 «Положення про систему забезпечення якості освіти та освітнього процесу в Київському національному університеті імені Тараса Шевченка».

Перелік навчальних дисциплін для вибіркової складової та робочі програми навчальних дисциплін представлені на офіційному сайті факультету комп'ютерних наук та кібернетики: <http://csc.knu.ua/uk/selected-subjects> та <http://csc.knu.ua/uk/programs>.

\*\* Вибірковий компонент ВК01 «Базова загальновійськова підготовка (теоретична частина)» обов'язково включається до індивідуального навчального плану громадян України, які навчаються за денною або дуальною формою здобуття освіти, і для яких, згідно із Законом України «Про військовий обов'язок і військову службу», проходження базової підготовки є обов'язковим.

## 2.2 Структурно-логічна схема ОП



### **3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ**

Атестація випускників освітньо-професійної програми «Інтелектуальні технології кіберзахисту» за спеціальністю F5 «Кібербезпека та захист інформації» здійснюється у формі захисту кваліфікаційної роботи бакалавра та єдиного державного кваліфікаційного іспиту й завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: Бакалавр з кібербезпеки та захисту інформації.

Єдиний державний кваліфікаційний іспит передбачає оцінювання рівня досягнення результатів навчання, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти, керуючись постановою Кабінету Міністрів України від 30 серпня 2024 р. № 1021. При захисті кваліфікаційної роботи перевіряється, наскільки досягнуто програмні результати навчання ПРН5, ПРН10, ПРН12, ПРН13, ПРН21.

Кваліфікаційна робота має передбачати розв'язок складного спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації.

Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.

Захист відбувається відкрито і публічно.

#### 4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ТА КОМПЕТЕНТНОСТЕЙ ОСВІТНЬОЇ ПРОГРАМИ

Програмні результати навчання	Компетентності																											
	Інтегральна	Загальні компетентності															Спеціальні (фахові) компетентності											
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	ЗК10	ЗК11	ЗК12	ЗК13	ЗК14	ЗК15	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12
ПРН1	+			+																								
ПРН2	+				+																							
ПРН3	+																											
ПРН4	+	+	+																									
ПРН5	+	+	+																									
ПРН6	+		+																									
ПРН7	+	+																										
ПРН8	+					+																						
ПРН9	+																											
ПРН10	+																											
ПРН11	+																											
ПРН12	+																											
ПРН13	+																											
ПРН14	+																											
ПРН15	+																											
ПРН16	+																											
ПРН17	+																											
ПРН18	+																											
ПРН19	+																											
ПРН20	+																											
ПРН21	+																											
ПРН22	+																											
ПРН23	+																											
ПРН24	+																											

## 5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ОК.01	ОК.02	ОК.03	ОК.04	ОК.05	ОК.06	ОК.07	ОК.08	ОК.09	ОК.10	ОК.11	ОК.12	ОК.13	ОК.14	ОК.15	ОК.16	ОК.17	ОК.18	ОК.19	ОК.20	ОК.21	ОК.22	ОК.23	ОК.24	ОК.25	ОК.26	ОК.27	ОК.28	ОК.29	ОК.30	ОК.31	ОК.32	ОК.33	ОК.34	ОК.35	ОК.36	ОК.37	ОК.38	ВК.01					
ЗК1					+		+		+				+	+	+	+		+	+	+	+		+	+	+				+			+				+								
ЗК2									+						+		+	+				+	+			+		+				+						+						
ЗК3		+			+												+																											
ЗК4						+	+																																					
ЗК5		+	+							+	+	+	+											+	+					+		+												
ЗК6	+			+	+																																							
ЗК7	+			+	+																																							
ЗК8	+	+		+				+									+																											
ЗК9																																									+			
ЗК10			+					+	+	+	+	+						+	+	+	+		+			+	+		+										+					
ЗК11			+					+	+	+	+	+			+		+											+							+	+				+				
ЗК12	+	+		+													+																											
ЗК13					+																																							
ЗК14									+																																			
ЗК15	+			+					+																																			
СК1					+																		+																					
СК2													+		+	+							+		+															+	+			
СК3								+																																				
СК4																+	+						+			+			+												+	+		
СК5													+				+						+			+			+											+	+			
СК6														+								+	+																					
СК7																																												
СК8																																												
СК9														+									+																					
СК10												+				+	+						+																			+		
СК11																													+														+	
СК12																													+														+	

## 6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (ПРН) ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

	ОК.01	ОК.02	ОК.03	ОК.04	ОК.05	ОК.06	ОК.07	ОК.08	ОК.09	ОК.10	ОК.11	ОК.12	ОК.13	ОК.14	ОК.15	ОК.16	ОК.17	ОК.18	ОК.19	ОК.20	ОК.21	ОК.22	ОК.23	ОК.24	ОК.25	ОК.26	ОК.27	ОК.28	ОК.29	ОК.30	ОК.31	ОК.32	ОК.33	ОК.34	ОК.35	ОК.36	ОК.37	ОК.38	ВК.01		
ПРН1		+			+												+																								
ПРН2						+	+																																		
ПРН3				+	+																			+																	
ПРН4	+							+	+	+	+	+			+		+			+				+				+													
ПРН5			+					+	+	+	+	+					+	+			+				+			+												+	
ПРН6			+								+				+						+				+																
ПРН7													+					+						+			+														
ПРН8								+	+	+	+			+				+						+			+														
ПРН9															+								+					+		+	+										
ПРН10													+			+					+	+					+		+		+							+	+		
ПРН11					+				+													+									+										
ПРН12																+						+										+	+							+	
ПРН13													+			+							+			+			+		+	+	+				+		+		
ПРН14																					+				+														+		
ПРН15								+																		+				+									+		
ПРН16																							+																		
ПРН17																																									
ПРН18																				+								+													
ПРН19																				+								+													
ПРН20															+														+												
ПРН21													+			+								+						+										+	
ПРН22																																									+
ПРН23																												+		+							+	+			
ПРН24																												+		+							+	+			

**Керівник проєктної групи:** Олена КАШПУР, декан факультету комп'ютерних наук та кібернетики, професор кафедри обчислювальної математики, доктор фізико-математичних наук

\_\_\_\_\_ « \_\_\_\_\_ » \_\_\_\_\_ 202\_\_ р.