ID 88975

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

«ЗАТВЕРДЖУЮ»
Ректор
_____ Володимир БУГРОВ
«23» березня 2026 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 «02» березня 2026 р.
протокол № 7

Введено в дію наказом ректора
від «23» березня 2026 за №111-32

Київ 2026 р.

ІНФОРМАЦІЯ ПРО ВНУТРІШНЮ ТА ЗОВНІШНЮ АПРОБАЦІЮ

Б. Рецензії представників академічної спільноти.

Анастасія ВАВІЛЕНКОВА, завідувач кафедри кібербезпеки центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України, доктор технічних наук, професор.

Позитивна рецензія від 22 вересня 2025 року. Зауважила, що мета освітньо-професійної програми «Інтелектуальні технології кіберзахисту», а саме підготовкка 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, - цілком відображає актуальні потреби у сфері кіберзахисту. Також відзначила наявність в ОПП таких освітніх компонентів, як «Криптографічний та стеганографічний захист інформації», «Основні положення інформаційної та кібернетичної безпеки», «Управління кіберризиками» та «Штучний інтелект в кіберзахисті», що дасть змогу здобувачам вивчити та дослідити не лише мотодологію побудови інтелектуальних технологій, але й набути знань щодо їх використання у сфері кіберзахисту.

Володимир МОХОР, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, член-кореспондент НАН України, доктор технічних наук, професор.

Позитивна рецензія від 03 жовтня 2025 року. Відмітив, що ОПП «Інтелектуальні технології кіберзахисту» передбачає підготовку саме різнопланових фахівців, що мають глибокі знання не лише у сучасних підходах до захисту інформації, а і вільно володіють загальним принципами та підходами до побудови комплексного програмного забезпечення, створення різноманітних систем штучного інтелекту, а також аналізу ситуації в реальному часі. Програма має чітку структуру, сформована за всіма міжнародними вимогами та рекомендаціями. Логічна послідовність дисциплін дозволить здобувачам вільно опанувати різноманітні напрямки, включаючи спеціальні розділи математики, передбачає ґрунтовну алгоритмічну та програмістську підготовку, а також напрацювання навичок використання методів штучного інтелекту та машинного навчання для проектування і створення новітніх систем кіберзахисту.

В. Відгуки представників професійних асоціацій.

Олександр КОРЧЕНКО, Президент громадської організації «Асоціація спеціалістів кібербезпеки», член-кореспондент НАН України, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, Заслужений діяч науки і техніки України.

Позитивна рецензія від 07 жовтня 2025 року. Зазначив, що програма має чітку та логічну структуру, перелік дисциплін та послідовність їх вивчення дозволить здобувачам вищої освіти отримати необхідні знання та компетенції у різних галузях інформаційних технологій, починаючи з основ побудови алгоритмів та аналізу вимог до програмного забезпечення, та закінчуючи використанням підходів штучного інтелекту та аналітичних систем, що базуються на обробці великих масивів даних. Таким чином, випускники стануть висококласними фахівцями та будуть затребувані на ринку праці не лише найближчим часом, а і у майбутньому.

Г. Відгуки представників ринку праці.

Олександр КУРІННИЙ, директор ТОВ «АКСОНСОФТ».

Позитивна рецензія від 23 вересня 2025 року. Відмітив, що з точки зору предметів та дисциплін, що вивчатимуться в рамках програми, слід відзначити значну кількість фундаментальних дисциплін, що включають математичний базис, побудову алгоритмів та основи штучного інтелекту. Це дозволить майбутнім фахівцям здійснювати аналіз кіберзагроз, оперативно реагувати, опанувати будь яке існуюче програмне забезпечення, модифікувати його та створити нове.

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)
Керівник проєктної групи						
КАШПУР Олена Федорівна	Декан факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка	Київський державний університет імені Т. Шевченка (1992, прикладна математика, математик)	Доктор фізико-математичних наук, 01.05.02 - Математичне моделювання 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.)	28 років	Виконавиця міжнародного грантового проєкту "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. Kashpur O., Boichenko B., Boychuk A. Fast Polynomial Reconstruction, PDMU-2025, XL International Conference ROBLEMS OF DECISION MAKING UNDER UNCERTAINTIES. 2. Kashpur O. F. Hermite Interpolation Polynomial for Functions of Several Variabl // Cybernetics and Systems Analysis. - 2022. - Vol. 58, Iss. 3. P. 399 - 408. 3. Кашпур О. Ф. Фундаментальні поліноми інтерполяційної формули Ерміта в лінійному нормованому та в евклідових просторах // Журнал обчислювальної та	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 проєкту Erasmus+Jean Monnet Module 101085516-QMSEEI – ERASMUS-JMO – 2022 HEI – TCH-

					прикладної математики. - 2022. - № 2. С. 50 - 58. 4. 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. 5. Макаров В. Л., Кашпур О. Ф. Огляд теорії поліноміальної інтерполяції // Український математичний журнал - 2025., т. 77 - №7. С. 461 – 488.	RSCH. Київський національний університет імені Тараса Шевченка, 10-12.2024, «Стрес-менеджемент та техніки психологічної самопідготовки», KU 02070944/0011987-24. CERTIFICATE, The University of L'Aquila (International Credit Mobility), 15.02.2025.
Члени проєктної групи						
ЗАВАДСЬКИЙ Ігор Олександрович	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	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 1. Zavadskyi I.O., Lossless text compression by means of binary-coded ternary number representation. Discrete Applied Mathematics, vol. 354, p. 15–22, 2024. 2. Zavadskyi, I., Kovalchuk, M. Binary Mixed-Digit Data Compression Codes. SPIRE. Lecture Notes in Computer Science, vol 14240, pp. 381–392, 2023.	Курси підвищення кваліфікації «Information Security Risk Management Review course» в ISACA Kyiv Center, диплом від 25.11.2022. Стажування «Викладання фізико-математичних дисциплін із використанням цифрових інструментів», сертифікат № PhmSI-010402-KSW від 12.05.2024

КОВАЛЬЧУК Людмила Василівна	Провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України	Київський державний університет ім. Т. Шевченка (1989 р., математика, математик-викладач)	Доктор технічних наук, 05.13.21 – Системи захисту інформації (ДД № 007369, 28.04.2009р.), спецтема, професор кафедри інформаційних систем (АП № 000261, 12.12.2017р.)	34 роки	Автор понад 150 публікацій, з них 49 проіндексовані в наукометричній базі Scopus, 1 монографія, 7 навчальних посібників. Основні публікації: 1. Kovalchuk, L., Rodinko, M., Oliynykov, R. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2023, pp. 275–293. https://www.scopus.com/record/display.uri?eid=2-s2.0-85149863201&origin=resultslist 2. Kovalchuk, L.V., Vykhlo, A.A. Estimation of the Probability of Success of a Frontrunning Attack on Smart Contracts. Cybernetics and Systems Analysis, 60, 881–890 (2024). https://doi.org/10.1007/s10559-024-00725-z 3. Kovalchuk, L.V., Kuchynska, N.V., Kondratenko, M.S. Determining the Number of Confirmation Blocks in a Two-Level Blockchain with Proof-of-Proof Consensus Protocol for Different Consensus Types in Mainchain/Sidechain to Prevent Double Spend Attack. I. PoS in Mainchain and PoW in Sidechain. Cybernetics and Systems Analysis, 60, 646–655 (2024). https://doi.org/10.1007/s10559-024-00703-5 4. Kovalchuk, L., Davydenko, A., Klymenko, T., Nedashkivska, A., Hilgurt, S. Development of an algorithm with temporary cryptographic security for encrypting	ISACA Kyiv Chapter, "Information security risk management review course", 180 годин, 25.11.2022.

					video stream from an unmanned aerial vehicle. Eastern-European Journal of Enterprise Technologies. Vol. 5, No. 9 (137), 2025, pp. 41–53. https://doi.org/10.15587/1729-4061.2025.340917 Керівник докторантів та аспірантів, кваліфікаційних та курсових робіт здобувачів освіти.	
КУДІН Антон Михайлович	Головний експерт управління безпеки інформації Департаменту безпеки Національного банку України, професор кафедри математичних методів захисту інформації Фізико-технічного інституту НТУУ «КПІ імені Ігоря Сікорського)	Київське вище інженерне радіотехнічне училище ППО ім. маршала авіації Покришкіна О.І., (1993, математичне забезпечення автоматизованих систем управління, інженер-математик)	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.)	32 роки	Керівник міжнародного грантового проєкту (НТУУ «КПІ імені Ігоря Сікорського та USAID) «Розподілена система раннього виявлення вторгнень та оцінки кібербезпеки» (№ G -202102-67499, 19.07.2021). 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. https://doi.org/10.3390/electronics12030721 2. V. Tkach, A. Kudin, V. Zadiraka, I. Shvidchenko Signatureless anomalous behavior detection in information systems / Кібернетика та системний аналіз. – 2023. – Т.59. - № 5. – С.100-112. https://doi.org/10.1007/s10559-023-00613-y 3. Кудін А.М., Кудін І.А., Чіхладзе В.З. Застосування загальної теорії оптимальних алгоритмів в криптографії, стега-нографії та блокчейн-технології / Кібернетика та системний аналіз. – 2025. – Т.61. - № 4. – С.46-57. https://doi.org/10.34229/kca2522-9664	Член-кореспондент Національної Академії Наук України за спеціальністю «Кібербезпека» (2024)

ПАНЧЕНКО Тарас Володимирович	Завідувач кафедри теорії та технології програмування Київського національного університету імені Тараса Шевченка	Київський національний університет імені Тараса Шевченка (2001, інформатика, магістр інформатики)	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)	22 роки	Керівник міжнародного грантового проєкту "Cybersecurity Seminar Program" у партнерстві з Google.org та Virtual Routes 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.	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

КАРНАУХ Тетяна Олександрівна	Доцент кафедри теоретичної кібернетики Київського національного університету імені Тараса Шевченка	Київський національний університет імені Тараса Шевченка (1997, прикладна математика, математик, викладач математики та інформатики)	Кандидат фізико-математичних наук, 01.01.08 - Математична логіка, теорія алгоритмів і дискретна математика (ДК № 034851 від 08.06.2006 р.), "Класи функцій та чисел, що визначаються трансформаційними та генеруючими моделями обчислень", доцент кафедри теоретичної кібернетики (12ДЦ № 022695 від 21.05.2009 р.)	24 роки	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 С++" (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-можливісний підхід до задач розпізнавання", "Qualitative estimation of plagiarism presence in programming assignment submissions". Бере участь у міжнародних конференціях, керівник дипломних та курсових робіт студентів.	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, https://certs.prometheus.org.ua/cert/7379602b848d4fc6acf6e817d1c7d76a). SoftServe Academy course "Tech Summer Bootcamp for Teachers" (10 годин, 2023, Серія ІА № 14501/2023). W3Cx Professional Certificate via edX "Front-End Web Developer" (2022, https://credentials.edx.org/credentials/689418ae3d5f4f3289b7e0470ab21cf6/). Coursera certificate "Introduction to Software Testing" (30 годин, 2023, https://coursera.org/verify/4RE9ZYSMPHHB). Coursera Professional Certificate "Google IT Automation with Python" (coursera.org/verify/professional-cert/VM7VFQW93EHW, 2020). Етико-психологічне забезпечення реалізації куратором ЗВО завдань освітньо-професійної соціалізації та патріотичного виховання студентів (10-22 січня 2024 року, 1 кредит, KU 02070944/000061-24) Психолого-педагогічний супровід психологічної компетентності спеціалістів ЗВО (10-31 травня 2023 року, 1 кредит, KU 02070944/000839-23) SoftServe Academy "CLOUD ENVIRONMENT CONFIGURATION AND SECURITY" 15 лютого 2024 – 16 квітня 2024 XN № 17860/2024 , April 16, 2024, 4 кредити.

СУПРУН Ольга Миколаївна	Доцент кафедри теорії та технології програмування Київського національного університету імені Тараса Шевченка	Київський державний університет ім. Т. Шевченка (1983, прикладна математика, математик)	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)	32 роки	Виконавиця міжнародного грантового проєкту "Cybersecurity Seminar Program" у партнерстві з Google.org та Virtual Routes. Член групи розробників 9 професійних стандартів в сфері інформаційної безпеки та кібербезпеки, зокрема: Фахівець сфери захисту інформації; Фахівець з технічного захисту інформації; Фахівець з криптографічного захисту інформації; Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту. Бере участь у міжнародних конференціях, автор більше 80 публікацій. Основні публікації: 1.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 & Conflict Management in Global Information Networks (CH&CMiGIN 2024), Kyiv, Ukraine, January 24–27, 2024. P. 35-46. https://ceur-ws.org/Vol-3925/paper04.pdf 2. Olha Suprun Oleksandr Provotar, Oleh Suprun. Development of modern payment gateways using blockchain technology: Proceedings of the Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, (CH&CMiGIN 2025), Kyiv, Ukraine, June 20–22, 2025. P. 59-68. http://ceur-ws.org/Vol-4024/	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). 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 КПІ ім. Ігоря Сікорського, січень 2025, 1 кредит ЄКТС (сертифікат 7ee684bb-1b41-4395-bd6a-e3ed783776ae).

					3. Lemesheva N. Antonenko H, Halachev P, Suprun O, Tytarchuk Y. The impact of quantum computing on the development of algorithms and software. Data and Metadata [Internet]. 2024 Oct. 3 [cited 2026 Feb. 15];3:.242. Available from: https://dm.ageditor.ar/index.php/dm/article/view/242	
ФІСУНЕНКО Андрій Леонідович	Директор ТОВ «САМСУНГ РнД 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 геометрічних об'єктів із заданими властивостями на площині»	31 рік	Автор 12 публікацій та тез конференцій, 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 іновації»: 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	Підвищення кваліфікації, НТУУ «Київський Політехнічний інститут», Фізико-технічний інститут, Центр перепідготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки. Свідотво СПК АЕ №199629, напрям «Організація захисту мовної інформації у телекомунікаційних мережах і системах зв'язку».

ШАРАПОВ Михайло Михайлович	Доцент кафедри прикладної статистики Київського національного університету імені Тараса Шевченка	Київський національний університет імені Тараса Шевченка, (1995, математика, математик, викладач (ЛВ ВЕ 002931))	Кандидат фізико-математичних наук, 01.01.06 - Теорія ймовірностей і математична статистика (ДК 004591, 13.10.1999), «Граничні теореми для оцінок параметрів випадкових процесів полів із довгою пам'яттю та їх уточнення», доцент кафедри прикладної статистики (12 ДЦ № 017127, 21.06.2007)	26 років	Учасник міжнародних комітетів зі стандартизації SC 27 (Підкомітет 27, Інформаційна безпека, кібербезпека та захист конфіденційності) та SC 39 (Підкомітет 39, Екологічна ефективність IT); уповноважений голосуючий та спостерігач від України (SE UkrNDNC) щодо проєктів міжнародних стандартів (DIS та FDIS) у комітетах ISO/IEC JTC 1/SC 27 та ISO/IEC JTC 1/SC 39. Автор понад 25 науково-дослідних робіт, з них 1. Eugene Lebedev, Mykhailo Sharapov, Optimization Problems for Retrial Queues with Unreliable Server. Modern Optimization Methods for Decision Making Under Risk and Uncertainty. First edition. / edited by Alexei A. Gaivoronski et al. - Boca Raton: CRC Press, 2023. pp. 360-371, doi 9781003260196-16 Автор 11 навчально-методичних посібників, 8 науково-популярних статей, 17 стандартів України.	Підвищення кваліфікації "SSWU: Teachers' Smart Up: Summer Edition 2024", 30 годин (1 ECTS), сертифікат ID aea4ca23b1c74d67bd0af420192fdfc7.

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»

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

3 - Характеристика освітньої програми	
Опис предметної області (галузь знань / спеціальність / спеціалізація програми)	**Об'єкти вивчення:** - технології кібербезпеки та захисту інформації; - процеси управління кібербезпекою та захистом інформації; - об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Цілі навчання:** підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. **Теоретичний зміст предметної області:** 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. **Методи, методики та технології:** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** 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).
Орієнтація освітньої програми	Освітньо-професійна академічна.
Основний фокус освітньої програми та спеціалізації	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.
Особливості програми	Освітній процес включає вивчення інтелектуальних технологій, зокрема методів штучного інтелекту, машинного навчання для виявлення та запобігання складним кіберзагрозам.

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть здійснювати професійну діяльність в органах державної влади та місцевого самоврядування, у суб'єктах сектору безпеки і оборони, у фінансових установах, телекомунікаційних компаніях, IT-компаніях та інших організаціях державної, комунальної й приватної форм власності, у підрозділах, що забезпечують функціонування систем кібербезпеки та захисту інформації. Випускники можуть обіймати посади початкового рівня у сфері кібербезпеки та захисту інформації, зокрема фахівця з інформаційної безпеки, фахівця з кібербезпеки, аналітика з моніторингу подій інформаційної безпеки, адміністратора систем і засобів захисту інформації, фахівця з управління вразливостями та тестування захищеності інформаційно-комунікаційних систем. Професійна діяльність пов'язана з моніторингом і аналізом подій безпеки, первинним реагуванням на інциденти, впровадженням і супроводом систем управління інформаційною безпекою, налаштуванням та експлуатацією засобів програмного захисту інформації, оцінювання ризиків і вразливостей, застосуванням інтелектуальних методів виявлення та аналізу кіберзагроз.
Подальше навчання	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	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, проєктно-орієнтоване навчання.
Оцінювання	Письмові та усні іспити, звіти до лабораторних робіт, усні презентації, поточний контроль, заліки, диференційовані заліки, захист кваліфікаційної роботи бакалавра та єдиний державний кваліфікаційний іспит.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях.

компетентності (ЗК)	**ЗК2.** Знання та розуміння предметної області і розуміння професійної діяльності. **ЗК3.** Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК4.** Здатність спілкуватися іноземною мовою. **ЗК5.** Здатність вчитися і оволодівати сучасними знаннями. **ЗК6.** 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. **ЗК7.** Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК8.** 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. **ЗК9**[1]**.** Здатність захищати Батьківщину. **ЗК10.** Здатність до абстрактного мислення, аналізу та синтезу. **ЗК11.** Здатність виявляти, ставити та вирішувати проблеми. **ЗК12.** Цінування та повага різноманітності та мультикультурності. **ЗК13.** Здатність виявляти ініціативу та підприємливість. **ЗК14.** Прагнення до збереження навколишнього середовища. **ЗК15.** Здатність діяти соціально відповідально та свідомо.
Спеціальні компетентності	**СК1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. **СК2.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. **СК3.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. **СК4.** Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. **СК5.** Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. **СК6.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) **СК7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. **СК8.** Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **СК9.** Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. **СК10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози

	інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. **СК11.** Здатність використовувати методи штучного інтелекту, машинного навчання для виявлення, класифікації та прогнозування кіберзагроз. **СК12.** Здатність оцінювати ефективність інтелектуальних технологій кіберзахисту, враховуючи їх вплив на безпеку, продуктивність і стійкість інформаційних систем.
7 – Програмні результати навчання	
Програмні результати навчання	**ПРН1.** Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. **ПРН2.** Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. **ПРН3.** Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. **ПРН4.** Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. **ПРН5.** 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. **ПРН6.** Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. **ПРН7.** 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. **ПРН8.** Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. **ПРН9.** Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. **ПРН10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. **ПРН11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. **ПРН12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. **ПРН13.** 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. **ПРН14.** 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. **ПРН15.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. **ПРН16.** Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. **ПРН17.** 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. **ПРН18.** Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **ПРН19.** Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. **ПРН20.** 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. **ПРН21.** 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. **ПРН22[2].** Опанувати базові загальновійськові знання та вміння, необхідні для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України. **ПРН23.** Застосовувати методи машинного навчання, штучного інтелекту та нейронних мереж для побудови моделей виявлення, прогнозування та запобігання кіберзагрозам. **ПРН24.** Виконувати впровадження інтелектуальних технологій в системи інформаційної безпеки організації та оцінювати їх.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	До освітнього процесу долучені викладачі, що є професіоналами практиками галузі кібербезпеки та захисту інформації.
Специфічні характеристики матеріально-	Здобувачі освіти мають доступ до лабораторії штучного інтелекту, яка функціонує на факультеті комп'ютерних наук та кібернетики.

технічного забезпечення	
Специфічні характеристики інформаційного та навчально-методичного забезпечення	Використання електронної бібліотеки факультету комп'ютерних наук та кібернетики (http://csc.knu.ua/uk/library) та авторських розробок науково-педагогічних працівників факультету.
9 – Академічна мобільність	
Національна кредитна мобільність	–
Міжнародна кредитна мобільність	–
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів здійснюється на загальних умовах.

[1] 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.

[2] 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
Обов'язкові компоненти ОП			
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	Основи екології	2	Залік
ОК.10	Дискретна математика	4	Іспит
ОК.11	Алгебра	4	Іспит
ОК.12	Математичний аналіз	10	Іспит
ОК.13	Програмування	10	Іспит
ОК.14	Вступ до спеціальності	3	Залік
ОК.15	Групова динаміка та комунікація	3	Залік
ОК.16	Математичні основи криптології	5	Іспит
ОК.17	Дискретні структури та алгоритми	5	Іспит
ОК.18	Фізичні основи захисту інформації	5	Залік
ОК.19	Теорія ймовірностей та математична статистика	5	Іспит
ОК.20	Архітектура обчислювальних систем	3	Залік
ОК.21	Комп'ютерні мережі	4	Іспит
ОК.22	Криптографічний захист інформації	4	Іспит
ОК.23	Нормативно-правове забезпечення кібербезпеки та захисту інформації	3	Залік
ОК.24	Теорія інформації та кодування	4	Залік
ОК.25	Операційні системи	5	Іспит
ОК.26	Стеганографія	4	Іспит
ОК.27	Технічні системи захисту інформації	5	Залік
ОК.28	Управління кіберризиками	5	Іспит
ОК.29	Бази даних	3	Іспит
ОК.30	Засоби забезпечення безпеки в комп'ютерних і мережевих системах	4	Іспит
ОК.31	Низькорівневі вразливості програмного забезпечення	4	Залік
ОК.32	Системи управління інформаційною безпекою	6	Іспит
ОК.33	Хмарні технології та кібербезпека	4	Іспит

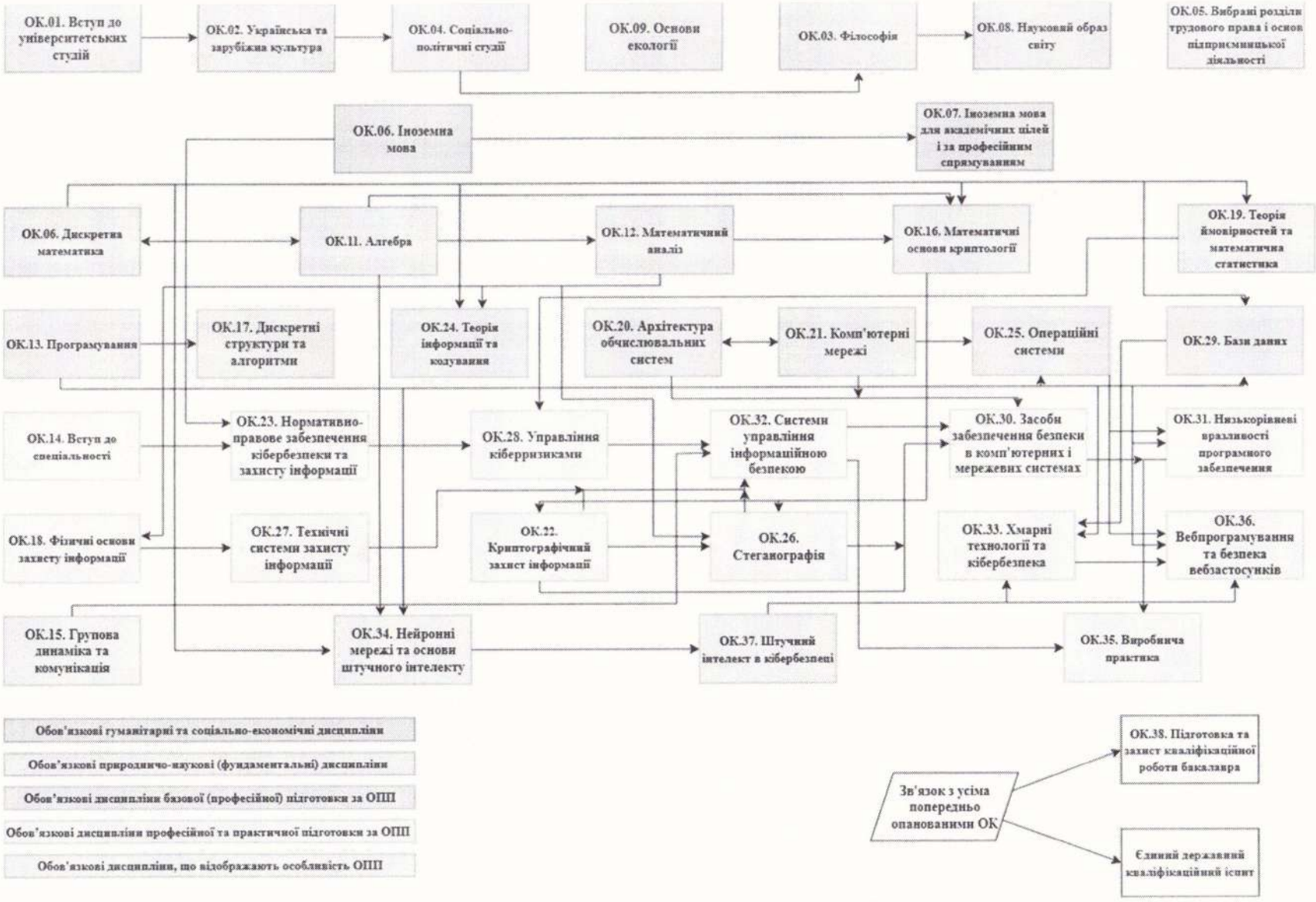
ОК.34	Нейронні мережі та основи штучного інтелекту	5	Іспит
ОК.35	Виробнича практика	6	Диф.залік
ОК.36	Вебпрограмування та безпека вебзастосунків	7	Іспит
ОК.37	Штучний інтелект в кіберзахисті	5	Іспит
ОК.38	Підготовка та захист кваліфікаційної роботи бакалавра	6	Захист
Загальний обсяг обов'язкових компонент:		**177,0**	
Вибіркові компоненти ОП*			
Вибір з переліку**			
	Здобувач освіти може обрати навчальні дисципліни з запропонованих переліків	60	Заліки, іспити
	До одного з переліків обов'язково включається дисципліна[3]:		
ВК.01[1]	Базова загальновійськова підготовка (теоретична частина)	3	Диф.залік
Загальний обсяг вибіркових компонент:		**63**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

* 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.

[3] Вибірковий компонент ВК.01[1] «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 ПРН4, ПРН5, ПРН6, ПРН7, ПРН10, ПРН12, 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

«13» 10 2025 р.