МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

«ЗАТВЕРДЖУЮ»
Ректор
Київського національного університету
імені Тараса Шевченка
_____ Володимир БУГРОВ
«__» червня 2025 р.

СЕРТИФІКАТНА ПРОГРАМА

«ОСНОВИ КІБЕРБЕЗПЕКИ МАЛИХ ОРГАНІЗАЦІЙ»

У межах першого (бакалаврського), другого (магістерського) рівнів вищої освіти

за спеціальністю: **F5 «Кібербезпека та захист інформації»**
галузі знань: **F «Інформаційні технології»**

Розглянуто та затверджено
на засіданні Вченої ради
від «02» червня 2025 р.
протокол № 12

Введено в дію наказом ректора
від «19» червня 2025 р. за № 560-32

Київ 2025 р.

ПІДСТАВИ ДЛЯ РОЗРОБЛЕННЯ ПРОГРАМИ

За даними ЄС, з 2022 року нестача фахівців з кібербезпеки в регіоні становила від 260 000 до 500 000 осіб, що є значним ризиком для безпеки Європи, тому існує нагальна потреба в збільшенні кількості випускників освітніх програм у цій галузі, та розробці нових програм, адаптованих до сучасних потреб. Аналогічна ситуація у США та інших регіонах. За дослідженями провідних консалтингових компаній та Даоського Економічного Форуму у світі критично не вистачає фахівців з кібербезпеки, і ця потреба буде лише зростати. Дефіцит кадрів у галузі складає кілька мільйонів спеціалістів. В Україні потреба у фахівцях з кіберзахисту відчувається особливо гостро, адже з 2021 року значно зросла кількість кібератак (зокрема, на критичну інфраструктуру), і продовжує експоненційно збільшуватись.

Кібербезпека є перспективним і актуальним напрямком галузі «Інформаційні технології». Особливо гостро постає питання захисту інформаційної діяльності малих організації в умовах постійних кібератак та інформаційних провокацій. Актуальність програми обумовлена жорсткою політикою кіберворога та обмеженими матеріальними, організаційними і технічними можливостями локальних та громадських організацій. Тому розроблення сертифікатної програми «Основи кібербезпеки малих організацій» зумовлено необхідністю та доцільністю впровадження професійних компетентностей фахівців, професійна діяльність яких пов'язана з організацією кібербезпеки, налагодженням процесу кіберзахисту, пошуком вразливостей інформаційних систем та формуванням вказівок щодо оптимізації кіберзабезпеки в малих організаціях, які не можуть собі дозволити підтримку відділів захисту інформації та оплачувані послуги кваліфікованих фахівців з кібербезпеки.

ІНФОРМАЦІЯ ПРО ЗОВНІШНЮ АПРОБАЦІЮ

А. Відгуки кафедр / загальноуніверситетських підрозділів.

Б. Рецензії представників академічної спільноти.
Рецензія доктора технічних наук (05.13.21 «Системи технічного захисту інформації»), професора, проректора з наукових досліджень та трансферу технологій Державного університету «Київський авіаційний університет» *Сергія ГНАТЮКА*
Дата рецензування: «19» 05 2025 р. Рецензія позитивна.

В. Відгуки представників професійних асоціацій.
Відгук президента громадської організації «Асоціація спеціалістів кібербезпеки», член-кореспондента НАН України, доктора технічних наук, професора, лауреата Державної премії України в галузі науки і техніки, Заслуженого діяча науки і техніки України *Олександра КОРЧЕНКА*
Дата надання відгуку: «12» 05 2025 р. Відгук позитивний.

Г. Відгуки представників ринку праці.
Відгук керівниці відділу інженерії безпеки (Head of security engineering) Cossack Labs *Анастасії ВОЙТОВОЇ*
Дата надання відгуку: «15» 05 2025 р. Відгук позитивний.

ПЕРЕДМОВА

Розроблено проєктною групою в складі:

Прізвище, ім'я, по батькові керівника та членів проєктної групи	Найменування посади (для сумісників - місце основної роботи, найменування посади)	Найменування закладу, який закінчив член проєктної групи (рік закінчення, спеціальність, кваліфікація)	Науковий ступінь, шифр і найменування наукової спеціальності, тема дисертації, вчене звання, за якою кафедрою (спеціальністю) присвоєно	Стаж наук.-пед. та/або наук. роб.	Інформація про наукову діяльність (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 члена проєктної групи (найменування закладу, вид документа, тема, дата видачі)
Керівник проєктної групи						
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)	К. ф.-м. н., 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 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	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

					Communications Technologies. – Springer Nature Switzerland, Cham. – 2023. – Vol. 180. – pp. 321–333. 3. T.Panchenko, M.Kovalchuk,V.Khar-chenko, 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.	
Члени проектної групи						
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)	К. ф.-м. н., 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),	28 років	Виконавиця 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 Держспецзв’язку 25 листопада 2022року №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 Держспецзв’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 Держспецзв’язку 23 січня 2024 року №38. С.28.	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" 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

МЕЖЕРИЦЬ-КА Юлія Ігорівна	Провідна інженерка з кібербезпеки (Lead Security Engineer) в Cossack Labs Limited	Київський національний університет імені Тараса Шевченка (2013, інформатика, каліфікація програміста системного, наукового співробітника (програмування), викладача вищого навчального закладу)	Не має	11 років	Колишня директорка Women Who Code Kyiv Голова спільноти Vona Tech Community Лідерка в OWASPZhytomyr	Сертифікація System Security Certified Practitioner від 23.04.2023, ISC2 № 932920

При розробленні програми враховані:

1. Стандарти: NIST CSF, ISO/IEC 27002, European Cybersecurity Skills Framework Role Profiles
2. Рекомендації представників галузі (Cossack Labs Limited, R&B Team LLC)
3. Частково враховано стандарт вищої освіти України спеціальності «Кібербезпека та захист інформації» (затверджений 29.10.2024 № 1547).

1. ПРОФІЛЬ СЕРТИФІКАТНОЇ ПРОГРАМИ

«ОСНОВИ КІБЕРБЕЗПЕКИ МАЛИХ ОРГАНІЗАЦІЙ» «FUNDAMENTALS OF CYBERSECURITY FOR SMALL ORGANIZATIONS»

зі спеціальності: F5 «Кібербезпека та захист інформації»
галузі знань: F «Інформаційні технології»

1 – Загальна інформація	
Опис часткової (мікро) кваліфікації	Часткове підвищення кваліфікації за сертифікатною програмою «*Основи кібербезпеки малих організацій»* Спеціальність: F5 «Кібербезпека та захист інформації» Галузь знань: F «Інформаційні технології»
Мова(и) навчання і оцінювання	Українська
Обсяг програми	6 кредитів ЄКТС (180 годин)
Тип програми	Сертифікатна програма
Повна назва структурного підрозділу у якому здійснюється навчання	Факультет комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка
Назва структурного підрозділу, який бере участь у забезпеченні програми	
Цикл/рівень програми	6, 7 рівень НРК України 6, 7 рівень EQF-LLL Перший, другий цикл QF-EHEA
Цільова аудиторія	Здобувачі вищої освіти КНУ імені Тараса Шевченка денної та заочної форми навчання та зовнішні слухачі
Умови доступу до програми	Повна загальна середня освіта або вища освіта ОР Бакалавр, ОКР Спеціаліст, ОР Магістр
Форма навчання	Очна, з використанням технологій дистанційного навчання
Документ що видається за результатами навчання	Сертифікат встановленого зразка КНУ імені Тараса Шевченка
Термін дії програми	5 років
Інтернет-адреса постійного розміщення опису програми	https://cybersecurity.knu.ua

2 – Мета програми	
Підготовка фахівців, здатних проводити теоретичні та експериментальні дослідження в галузі кібербезпеки та захисту інформації; застосовувати математичні методи й алгоритмічні принципи в моделюванні, проєктуванні, розробці та супроводі документації та рекомендацій з покращення кіберзахисту малих організацій; здійснювати розробку, впровадження і супровід рекомендацій з управління ризиками. Надати слухачам знання з кібербезпеки та розвинути практичні навички організації процесу кіберзахисту, пошуку вразливостей інформаційних систем та формування вказівок щодо оптимізації кіберзабезпеки в малих організаціях. Через навчання і подальше стажування, консультування місцевих громадських організацій, розвинути компетентності слухачів програми у сфері кібербезпеки та захисту інформації.	
3 - Характеристика програми	
Предметна область	Інформаційні технології / Кібербезпека та захист інформації ***Об'єкт вивчення:*** Процеси та засоби забезпечення кібербезпеки та інформаційного захисту в контексті захисту інформації окремих осіб і малих організацій, методи моделювання, проєктування, розробки та впровадження рішень із управління ризиками в галузі кіберзахисту. ***Цілі навчання:*** підготовка фахівців, здатних: реагувати на актуальні виклики інформаційного захисту окремих осіб і малих організацій; проводити практичні дослідження у сфері кіберзахисту; розробляти та впроваджувати стратегії управління ризиками в інформаційній безпеці для малих організацій. ***Теоретичний зміст предметної області:*** теоретичні засади кібербезпеки та захисту інформації, що включають основні принципи організації інформаційного захисту, деякі математичні методи аналізу та моделювання кіберзагроз, методології управління ризиками в інформаційній безпеці, підходи до створення рекомендацій щодо вдосконалення кіберзахисту малих організацій і окремих осіб. ***Методи, методики та технології:*** практичні методи дослідження в галузі кібербезпеки, методики оцінювання та управління ризиками, сучасні інформаційні технології для розроблення, впровадження та супроводу рекомендацій з покращення кіберзахисту малих організацій і захисту інформації окремих осіб. ***Інструменти та обладнання:*** спеціалізовані програмні засоби для моделювання кіберзагроз, системи управління інформаційною

	безпекою, інструменти для аналізу вразливостей і тестування на проникнення, засоби криптографічного захисту, стандартне комп'ютерне та мережеве обладнання.
Основний фокус програми	Програма орієнтована на інтенсивне здобуття знань з інформаційної безпеки, впровадження кібербезпекової складової в діяльність малих організацій в Україні, та отримання практичих навичок організації процесу кіберзахисту, пошуку вразливостей інформаційних систем та формування вказівок щодо оптимізації кіберзабезпеки в малих організаціях. Програма розвиває у слухачів компетентності у сфері кібербезпеки через практичне консультування місцевих громадських організацій, які потребують кращого рівня захисту від кіберзагроз.
Особливості програми	Програма має прикладний характер, відповідає актуальним викликам кіберзахисту та організації інформаційного захисту окремих осіб та малих організацій. Програма має інтенсивну навчальну складову, а також розвиває кібербезпекові компетентності слухачів через обов'язкове застосування засвоєних знань та набутих навичок на практиці у реальних ситуаціях.
4 – Викладання та оцінювання	
Викладання та навчання	Проблемно-орієнтоване викладання з використанням дистанційної платформи Zoom. Мультимедійні та інтерактивні лекції, лабораторні заняття, самостійна робота на основі посібників, конспектів, інтернет-джерел, нормативно-правових документів; самонавчання; групова та індивідуальна робота; практична робота.
Оцінювання	Поточний контроль – усне опитування, виступи перед аудиторією, виконання лабораторних робіт, тестовий контроль отриманих компетентностей. Підсумковий контроль – у формі заліку шляхом письмового (комп'ютерного) тестування. Відгук за результатами виконаної слухачем практичної роботи.
5 – Програмні компетентності	
Загальні компетентності (ЗК)	ЗК01. Здатність до абстрактного мислення, аналізу і синтезу. ЗК02. Здатність застосовувати знання й уміння у практичних ситуаціях. ЗК03. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

	ЗК04. Здатність працювати в команді. ЗК05. Здатність до адаптації та дії в новій ситуації. ЗК06. Здатність генерувати нові ідеї (креативність). ЗК07. Здатність виявляти, ставити та вирішувати проблеми. ЗК08. Здатність приймати обґрунтовані рішення.
Фахові компетентності (ФК)	ФК01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги і стандарти з метою здійснення діяльності в галузі кібербезпеки та захисту інформації. ФК02. Здатність до використання інформаційних технологій, сучасних методів і моделей кібербезпеки та систем захисту інформації. ФК03. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації. ФК04. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки). ФК05. Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи кіберзахисту. ФК06. Здатність до пошуку, систематичного вивчення та аналізу науково-технічної інформації, вітчизняного й закордонного досвіду, пов'язаного із застосуванням методів кіберзахисту. ФК07. Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних системах, що призначені для захисту інформації. ФК08. Розуміти правові, етичні та психологічні аспекти діяльності в галузі кіберзахисту. ФК09. Здатність формулювати та розв'язувати задачі у сфері кіберзахисту. ФК10. Здатність розуміти поняття та визначення, цілі та результати діяльності у сфері захисту інформації, зокрема діяльності підприємства/організації, пов'язані із захистом інформації та кібербезпекою.
6 – Програмні результати навчання	
ПРН01. Аналізувати, аргументувати, приймати рішення при розв'язанні спеціалізованих задач та практичних завдань у сфері кіберзахисту, відповідати за прийняті рішення. ПРН02. Використовувати знання й розуміння математики, фізики та інформатики в захисті інформації, формалізувати задачі галузі кібербезпеки та захисту інформації. ПРН03. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики безпеки інформації. ПРН04. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту. ПРН05. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.	

ПРН06. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних. ПРН07. Вміти оцінювати та забезпечувати якість виконуваних досліджень. ПРН08. Застосовувати на практиці етичні вимоги щодо організації кібербезпеки. ПРН09. Передбачати майбутні кібербезпекові загрози, тенденції, потреби та виклики в організації. ПРН10. Оцінювати і покращувати рівень кібербезпеки організації.	
7 – Ресурсне забезпечення реалізації програми	
Характеристики кадрового забезпечення	Освітні компоненти сертифікатної програми забезпечують провідні науково-педагогічні працівники, які мають відповідний науковий ступінь, фахівці-практики, експерти у галузі кібербезпеки та захисту інформації. Передбачено залучення співробітників міжнародних організацій, українських та закордонних компаній для читання лекцій та проведення майстер-класів.
Характеристики матеріально-технічного забезпечення	Використання в навчальному процесі аудиторного фонду факультету комп'ютерних наук та кібернетики з мультимедійним обладнанням. Використання електронної бібліотеки факультету комп'ютерних наук та кібернетики (http://csc.knu.ua/uk/library) та авторських розробок науково-педагогічних працівників факультету.

2. ПЕРЕЛІК КОМПОНЕНТ СЕРТИФІКАТНОЇ ПРОГРАМИ «Основи кібербезпеки малих організацій»

Код н/д	Компоненти сертифікатної програми	Кількість кредитів	Кількість годин	
			всього	у т.ч. ауд.
1	**2**	**3**	**4**	**5**
1 семестр				
ОК 1	Правила кібербезпеки та соціальна інженерія	0,1	3	2
ОК 2	Основні положення інформаційної безпеки та кібербезпеки	0,2	6	4
ОК 3	OSINT: основні принципи та безпечний пошук інформації в інтернеті	0,1	3	2
ОК 4	Криптографічний захист інформації	0,2	6	4
ОК 5	Основні поняття операційних систем	0,5	15	10
ОК 6	Комп'ютерні віруси та антивірусний захист	0,3	9	6
ОК 7	Поняття про локальну та глобальну комп'ютерні мережі	0,3	9	6
ОК 8	Вразливості веб безпеки	0,4	12	8
ОК 9	Етичний хакінг	0,6	18	12
ОК 10	Розрахунок та управління ризиками	0,3	9	6
Підсумкове оцінювання: комп'ютерне тестування				
Загальна кількість за 1 семестр		***3***	***90***	***60***
2 семестр				
ОК 11	Практична робота	3	90	
Загальна кількість за 2 семестр		***3***	***90***	
ЗАГАЛЬНИЙ ОБСЯГ ПРОГРАМИ		**6**	**180**	**60**

3. ПІДСУМКОВЕ ОЦІНЮВАННЯ СЛУХАЧІВ

Підсумкове оцінювання результатів навчання слухачів сертифікатної *програми «Основи кібербезпеки малих організації»* проводиться в два етапи, а саме:

- шляхом тестування за 100-бальною шкалою з оцінкою «зараховано» (60-100 балів) та «не зараховано» (менше 60 балів) в першому семестрі;

- у другому семестрі передбачається виконання практичної роботи на основі даних конкретних організацій.

Необхідною умовою отримання сертифікату є наявність позитивного відгуку від організацій, на базі яких було виконано практичну роботу. Підсумковий бал є балом за тестування в першому семестрі.

Навчання за сертифікатною програмою «Основи кібербезпеки малих організації» завершується видачею сертифіката встановленого зразка КНУ імені Тараса Шевченка про проходження навчання.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ СЕРТИФІКАТНОЇ ПРОГРАМИ

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11
ЗК01		+			+					+	
ЗК02		+						+			
ЗК03	+				+				+		+
ЗК04	+						+				
ЗК05		+		+						+	
ЗК06			+								+
ЗК07					+	+		+			
ЗК08		+					+				+
ФК01	+		+						+		+
ФК02	+			+		+		+			
ФК03		+								+	+
ФК04			+					+			
ФК05	+					+	+				+
ФК06					+				+		+
ФК07		+					+	+			+
ФК08				+					+	+	+
ФК09	+		+			+	+				+
ФК10				+							+

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

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11
ПРН 01	+					+		+			+
ПРН 02			+							+	+
ПРН 03	+			+		+		+			
ПРН 04			+		+				+		+
ПРН 05		+					+				+
ПРН 06				+				+		+	
ПРН 07		+			+				+		+
ПРН 08	+		+				+				+
ПРН 09				+						+	+
ПРН 10	+				+			+			+

Керівник проєктної групи:
завідувач кафедри теорії та технології програмування,
кандидат фізико-математичних наук, доцент _____ **Тарас ПАНЧЕНКО**