МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

«ЗАТВЕРДЖУЮ»

Ректор
_____Володимир БУГРОВ
«____» _____ 2024 р.

СЕРТИФІКАТНА ПРОГРАМА
«ОСНОВИ КІБЕРБЕЗПЕКИ МАЛИХ ОРГАНІЗАЦІЙ»

В межах першого рівня вищої освіти

(редакція від « »_____2024 р., затверджена рішенням Вченої ради)

за спеціальністю:
125 «Кібербезпека та захист інформації»
Галузі знань 12 «Інформаційні технології»

Розглянуто та затверджено
на засіданні Вченої ради
від «___» _____ 2024 р.
протокол № ___

Введено в дію наказом ректора від
«____» _____2024 за №____

Київ 2024 р.

ЛИСТ ПОГОДЖЕННЯ
сертифікатної програми
«Основи кібербезпеки малих організацій»

1.1 Науково-методична рада: протокол №_____ від «__»_____20___ р.

_____

(особливі умови, за наявності)

Голова науково-методичної ради _____

2.1 Науково-методичний центр організації навчального процесу:

_____

(особливі умови, за наявності)

Директор НМЦ _____ «__»_____20___ р.

3.1 Сектор моніторингу якості освіти:

_____

(особливі умови, за наявності)

Керівник сектору _____ «__»_____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 _____ Людмила ОМЕЛЬЧУК

Розроблено:

Гарант освітньої програми: Тарас ПАНЧЕНКО, кандидат фізико-математичних наук, завідувач кафедри теорії та технології програмування

_____ «__»_____20___ р.

ПІДСТАВИ ДЛЯ РОЗРОБЛЕННЯ ПРОГРАМИ

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 питання 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 може бути пов’язана з вирішенням питань організації кібербезпеки, налагодженню процесу кіберзахисту, пошуку вразливостей інформаційних систем та формуванню вказівок щодо оптимізації кіберзабезпеки в малих організаціях, які не можуть собі дозволити підтримку відділів захисту інформації.

ІНФОРМАЦІЯ ПРО ЗОВНІШНЮ АПРОБАЦІЮ

Рецензія доктора технічних наук (05.13.21 «Системи технічного захисту інформації»), професора, в.о. проректора з наукової роботи Національного авіаційного університету Сергія ГНАТЮКА

Рецензія президента громадської організації «Асоціація спеціалістів кібербезпеки», член-кореспондента НАН України, доктора наук, професора, лауреата Державної премії України в галузі науки і техніки, Заслуженого діяча науки і техніки України Олександра КОРЧЕНКА

Відгук керівниці відділу інженерії безпеки (Head of security engineering) Cossack Labs Анастасії ВОЙТОВОЇ

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Прізвище, ім'я, по батькові керівника та членів проєктної 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 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 викладача (найменування закладу, вид документа, тема, дата видачі)
1	2	3	4	5	6	7
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)	21 рік	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.	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

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),	27 років	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. Аналітик з безпеки інформаційно-телекомунікаційних систем. Професійний стандарт. Петрушкевич О., Безштанько В., Гнатюк С. та інші, всього 19 осіб. Затверджено Наказ Адміністрації Держспецзв'язку 25 листопада 2022року №715. С.39. 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.

МЕЖЕРИЦЬКА 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	10 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 Number 932920

При розробленні Програми враховані:
Стандарти: NIST CSF, ISO/IEC 27002, European Cybersecurity Skills Framework Role Profiles
Рекомендації представників галузі (Cossack Labs Limited, R&B Team LLC)

1. ПРОФІЛЬ СЕРТИФІКАТНОЇ ПРОГРАМИ «ОСНОВИ КІБЕРБЕЗПЕКИ МАЛИХ ОРГАНІЗАЦІЙ»

зі спеціальності

125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Опис часткової (мікро) кваліфікації	Часткове підвищення кваліфікації
Мова навчання і оцінювання	Українська
Обсяг освітньої програми	6 кредитів ЄКТС (180 годин)
Тип програми	Сертифікатна
Повна назва структурного підрозділу, у якому здійснюється навчання	Факультет комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка
Назва організації/закладу вищої освіти, який бере участь у забезпеченні програми	–
Цикл/рівень програми	У межах 6 рівня НРК
Цільова аудиторія	Посадові особи, керівники та спеціалісти підприємств, установ, організацій, здобувачі вищої освіти, які бажають покращити свої знання з кібербезпеки та отримати практичні навички організації процесу кіберзахисту, пошуку вразливостей інформаційних систем та формуванню вказівок щодо оптимізації кіберзабезпеки в малих організаціях
Умови доступу до програми	Наявність атестату про повну загальну середню освіту
Форма навчання	Змішана з використанням технологій дистанційного навчання
Документ, що видається за результатами навчання	Сертифікат
Термін дії програми	5 років
Інтернет-адреса постійного розміщення опису програми	http://csc.knu.ua/uk/curriculum
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	
3 - Характеристика програми	
Предметна область	Спеціальність 125 «Кібербезпека та захист інформації»
Основний фокус програми	Програма орієнтована на інтенсивне формування знань з інформаційної безпеки і впровадження кібербезпекової складової в діяльність малих організацій в Україні
Особливості програми	Програма має прикладний характер, відповідає актуальним викликам кіберзахисту

	та організації інформаційного захисту окремих осіб та малих організацій. Слухачами сертифікатної програми можуть бути як здобувачі освіти КНУ імені Тараса Шевченка, так і зовнішні слухачі
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 підручників, конспектів, інтернет-джерел, нормативно-правових документів; самонавчання; групова та індивідуальна робота; випускова 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. Захист випускової практичної роботи слухача.
5 – Програмні компетентності	
Загальні компетентності (ЗК)	ЗК01. Здатність до абстрактного мислення, аналізу і синтезу. ЗК02. Здатність формулювати та розв'язувати задачі у сфері кіберзахисту, застосовувати знання у практичних ситуаціях ЗК03. Здатність розуміти поняття та визначення, цілі та результати діяльності у сфері захисту інформації, зокрема діяльності підприємства/організації, пов'язані із захистом інформації та кібербезпекою. ЗК04. Здатність застосовувати знання й уміння у практичних ситуаціях. ЗК05. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК06. Здатність працювати в команді. ЗК07. Здатність до адаптації та дії в новій ситуації. ЗК08. Здатність генерувати нові ідеї (креативність) ЗК09. Вміння виявляти, ставити та вирішувати проблеми. ЗК10. 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.
6 – Програмні результати навчання	
Програмні результати навчання (ПРН)	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, фахівці-практики, експерти у галузі кібербезпеки та захисту інформації, які мають відповідний науковий ступінь. Передбачено залучення співробітників міжнародних організацій, українських та закордонних компаній для читання лекцій та проведення майстер-класів
Характеристики матеріально-технічного забезпечення	Використання в навчальному процесі аудиторнго фонду ФКНК з мультимедійним

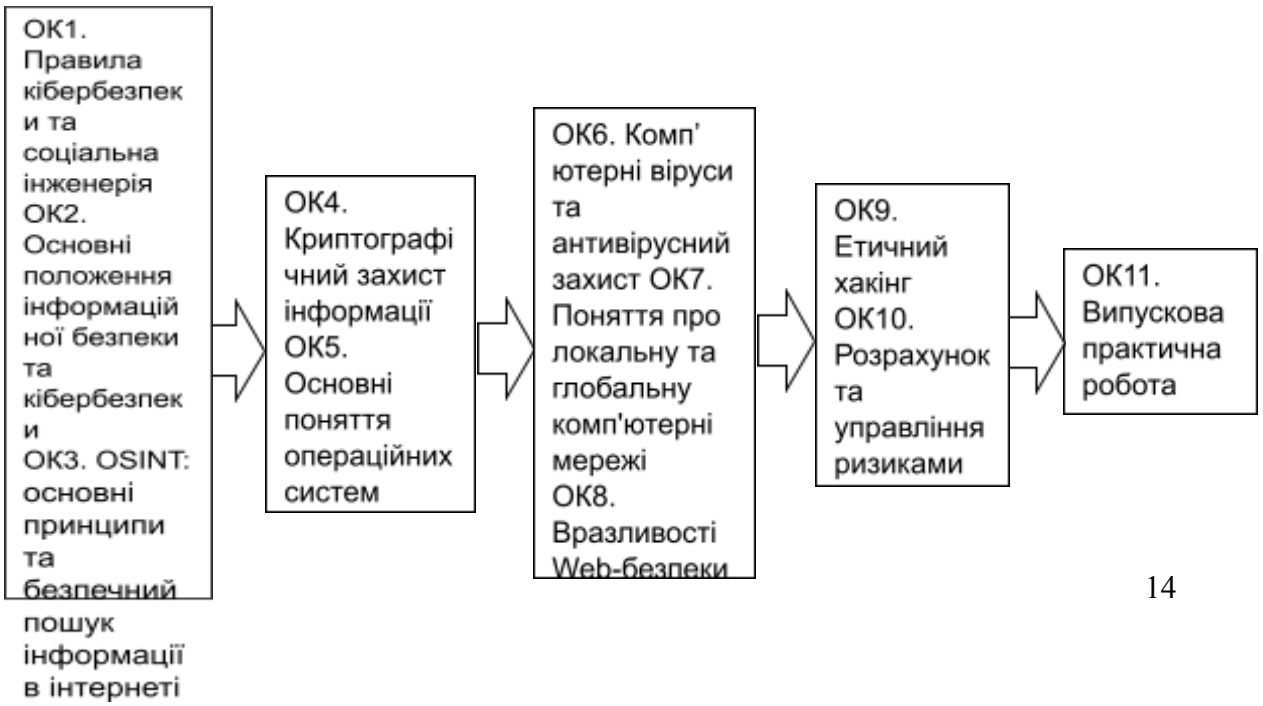
	обладнанням

2. ПЕРЕЛІК КОМПОНЕНТ СЕРТИФІКАТНОЇ ПРОГРАМИ «ОСНОВИ КІБЕРБЕЗПЕКИ МАЛИХ ОРГАНІЗАЦІЙ»

2.1 Перелік компонент СП

Код н/д	Компоненти програми	Кількість кредитів	Кількість годин	
			всього	у т.ч. ауд.
1	**2**	**3**	**4**	**5**
	1 семестр			
ОК.01	Правила кібербезпеки та соціальна інженерія	0,1	3	2
ОК.02	Основні положення інформаційної безпеки та кібербезпеки	0,2	6	4
ОК.03	OSINT: основні принципи та безпечний пошук інформації в інтернеті	0,1	3	2
ОК.04	Криптографічний захист інформації	0,2	6	4
ОК.05	Основні поняття операційних систем	0,5	15	10
ОК.06	Комп’ютерні віруси та антивірусний захист	0,3	9	6
ОК.07	Поняття про локальну та глобальну комп'ютерні мережі	0,3	9	6
ОК.08	Вразливості Web-безпеки	0,4	12	8
ОК.09	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	Випускова практична робота	3	90	
	Загальна кількість за 2 семестр	3	90	
	ЗАГАЛЬНИЙ ОБСЯГ ПРОГРАМИ	**6**	**180**	**60**

2.2 Структурно-логічна схема СП



3. ПІДСУМКОВЕ ОЦІНЮВАННЯ СЛУХАЧІВ

Підсумкове оцінювання результатів навчання слухачів сертифікатної програми «Основи кібербезпеки малих організації» проводиться шляхом тестування за G00GLE формою за 100-бальною шкалою з оцінкою «зараховано» (60-100% правильних відповідей) та «незараховано» (59 і менше % правильних відповідей) в першому семестрі.

В другому семестрі передбачається виконання випускної практичної роботи на основі даних конкретної організації.

Навчання за сертифікатною програмою «Основи кібербезпеки малих організації» завершується видачею сертифіката про підвищення кваліфікації.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ СЕРТИФІКАТНОЇ ПРОГРАМИ

ОК.01		+			+	+					+	+			+			
ОК.02	+			+			+			+			+				+	
ОК.03		+						+			+			+				
ОК.04			+				+					+						+
ОК.05	+				+				+							+		
ОК.06			+						+			+			+			
ОК.07		+				+				+								
ОК.08				+					+			+		+			+	
ОК.09					+											+		
ОК.10	+						+						+					+
ОК.11		+	+		+			+		+	+		+		+	+	+	

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

	ПРН01	ПРН02	ПРН03	ПРН04	ПРН05	ПРН06	ПРН07	ПРН08	ПРН09	ПРН10
ОК.01	+		+					+		+
ОК.02					+		+			
ОК.03		+		+				+		
ОК.04			+			+			+	
ОК.05				+			+			+
ОК.06	+		+							
ОК.07					+			+		
ОК.08	+		+			+				+
ОК.09				+			+			
ОК.10		+				+			+	
ОК.11	+	+		+	+		+	+	+	+

Керівник проєктної групи: _____**Тарас ПАНЧЕНКО**

_____ «_____»_____ 202__ р.