МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ЗАТВЕРДЖЕНО
Вченою радою університету
27 червня 2024 р., протокол № 8

Голова Вченої ради
_____Генаналій ПІВНЯК

ОСВІТНЬО-НАУКОВА ПРОГРАМА ВИЩОЇ ОСВІТИ
«Безпека кіберфізичних систем»

ГАЛУЗЬ ЗНАНЬ	12 Інформаційні технології
СПЕЦІАЛЬНІСТЬ	125 Кібербезпека та захист інформації
РІВЕНЬ ВИЩОЇ ОСВІТИ	Третій (освітньо-науковий)
СТУПІНЬ	Доктор філософії
ОСВІТНЯ КВАЛІФІКАЦІЯ	Доктор філософії з кібербезпеки та захисту інформації

Уводиться в дію з _01.09.2024р.
Наказ від 27 червня 2024р., № 19
В.о. ректора
_____Артем ПАВЛИЧЕНКО

Дніпро
НТУ «ДП»
2024

ЛИСТ-ПОГОДЖЕННЯ

Центр моніторингу знань та тестування
протокол № 3 від «12» 03 2024 р.
Директор _____ М.М. Одновол
(підпис, ініціали, прізвище)

Відділ внутрішнього забезпечення якості вищої освіти
протокол № 3 від «12» 03 2024 р.
Начальник відділу _____ О.О. Яворська
(підпис, ініціали, прізвище)

Навчально-методичний відділ
протокол № 3 від «12» 03 2024 р.
Начальник відділу _____ Ю.О. Заболотна
(підпис, ініціали, прізвище)

Завідувач аспірантури і докторантури _____ Л.О. Колісник
(підпис, ініціали, прізвище)

Науково-методична комісія спеціальності 125 Кібербезпека

Протокол № 7 від «27» 02 2024 р.

Голова науково-методичної комісії спеціальності _____ В.І. Корнієнко
(підпис, ініціали, прізвище)

Гарант освітньої програми _____ А.О. Корченко
(підпис, ініціали, прізвище)

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Корченко Анна Олександрівна – доктор технічних наук, професор, професор кафедри безпеки інформації та телекомунікацій (керівник робочої групи), гарант освітньо-наукової програми.
2. Іванченко Олег Васильович – доктор технічних наук, доцент, професор кафедри програмного забезпечення комп'ютерних систем.
3. Котух Євген Володимирович – доктор з державного управління, доцент, професор кафедри безпеки інформації та телекомунікацій.
4. Давиденко Кирило Олександрович– здобувач групи 125А-23-10.

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Євген Дон, директор Департаменту цифрової трансформації, інформаційних технологій та електронного урядування Дніпропетровської обласної державної адміністрації.
2. Юрій Пономаренко, начальник сектору захисту критичної інфраструктури Управління Держспецзв'язку у Дніпропетровській області, підполковник.

ЗМІСТ

ВСТУП

Освітньо-наукова програма розроблена на основі Постанови Кабінету Міністрів України від 23 березня 2016 р. № 261 «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)» із змінами від 03 квітня 2019 р. № 283 (далі Положення КМУ № 261) для третього (освітньо-наукового) рівня галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації.

Освітньо-наукова програма використовується під час:

– ліцензування спеціальності та акредитації освітньої програми;

– складання навчальних планів;

– формування робочих програм навчальних дисциплін, силабусів, програм практики, індивідуальних завдань;

– формування індивідуальних навчальних планів аспірантів;

– розроблення засобів діагностики якості вищої освіти;

– атестації аспірантів спеціальності 125 Кібербезпека та захист інформації;

– наукової орієнтації здобувачів фаху;

– зовнішнього контролю якості підготовки фахівців.

Користувачі освітньо-наукової програми:

– аспіранти, які навчаються в НТУ «ДП»;

– викладачі НТУ «ДП», які здійснюють підготовку аспірантів спеціальності 125 Кібербезпека та захист інформації;

Дія освітньої програми поширюється на кафедри університету, що беруть участь у підготовці фахівців ступеня доктора філософії спеціальності 125 Кібербезпека та захист інформації.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

1.1 Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний технічний університет «Дніпровська політехніка», відділ аспірантури та докторантури, кафедра безпеки інформації та телекомунікацій.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Доктор філософії Доктор філософії з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Безпека кіберфізичних систем
Тип диплому та обсяг освітньої програми	60 кредитів ЄКТС, термін навчання – 4 роки.
Наявність	Акредитація програми не проводилася.

акредитації	
Цикл/рівень	НРК України – 8, рівень FQ-EHEA – третій цикл, EQF-LLL – 8 рівень
Передумови	Особа має право здобувати ступінь доктора філософії за умови наявності в неї другого рівня вищої освіти. Особливості вступу на ОНП визначаються Правилами прийому до Національного технічного університету «Дніпровська політехніка», що затверджені Вченою радою
Мова(и) викладання	Українська
Термін дії освітньої програми	Термін не може перевищувати 4 роки та/або період акредитації. ОНП підлягає перегляду відповідно до змін нормативної бази України, але не рідше 1 разу на рік.
Інтернет-адреса постійного розміщення опису освітньої програми	Освітні програми НТУ «Дніпровська політехніка»: https://www.nmu.org.ua/ua/content/infrastructure/structural_divisions/science_met_dep/educational_programs/
1.2 Мета освітньої програми	
Підготовка на принципах академічної доброчесності, загальнолюдських цінностей, національної ідентичності та креативного становлення людини і суспільства майбутніх фахівців з кібербезпеки та захисту інформації із забезпеченням органічного поєднання освітньої та інноваційної діяльності, спрямованих на здобуття поглиблених теоретичних і практичних знань для продукування нових ідей та розв'язання складних комплексних проблем у галузі кібербезпеки та захисту інформації, оволодіння методологією наукової та педагогічної діяльності, а також проведення власного наукового дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.	
1.3 Характеристика освітньої програми	
Предметна область	12 Інформаційні технології / 125 Кібербезпека та захист інформації *Об'єкти вивчення та діяльності:* – проведення наукових досліджень, аналізу, створення та забезпечення функціонування інформаційних систем і технологій на об'єктах інформаційної діяльності та критичних інфраструктур сфери кібербезпеки та захисту інформації; – новітні системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – сучасні інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – автоматизовані системи управління інформаційною безпекою, кібербезпекою; – методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації. *Цілі навчання:* набуття здатності продукувати нові ідеї, розв'язувати комплексні проблеми в галузі професійної та дослідницько-інноваційної діяльності, а також здатності здійснювати науково-педагогічну діяльність у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики. *Теоретичний зміст предметної області:* принципи проведення наукових

	досліджень, теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі кібербезпеки та захисту інформації. *Методи, методики та технології:* сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення наукових та професійних задач в галузі кібербезпеки та захисту інформації. *Інструменти та обладнання:* програмно-апаратне та програмне забезпечення, інструментальні засоби, комп'ютерна техніка, спеціальні контрольно-вимірювальні прилади, програмно-технічні засоби автоматизації та системи автоматизації проектування, виробництва, експлуатації, контролю, моніторингу, мережні, мобільні, хмарні, технології, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі кібербезпеки та захисту інформації.
Орієнтація освітньої програми	Освітньо-наукова програма орієнтована на розв'язування комплексних задач із розробки моделей та засобів забезпечення кібербезпеки та захисту інформації.
Основний фокус освітньої програми	Освітньо-наукова програма спрямована на: розвиток теоретичної, методологічної та прикладної бази створення та забезпечення функціонування інформаційних технологій та кіберфізичних систем на об'єктах інформаційної діяльності та критичних інфраструктур у сфері кібербезпеки та захисту інформації; створення автоматизованих систем управління інформаційною безпекою на основі новітніх методів, моделей та засобів кібербезпеки та захисту інформації. Ключові слова: кібербезпека, інформаційна безпека, кіберфізичні системи, математичні методи кібербезпеки, системи і технології інформаційної та кібербезпеки та захисту інформації.
Особливості програми	Освітня програма передбачає поєднання теоретичних знань та практичну (у т.ч. викладацьку) підготовку і дозволяє здобувачам вищої освіти отримати навички щодо створення систем кібербезпеки та захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, кіберфізичних системах, проведення наукових досліджень у сфері кібербезпеки та захисту інформації.
1.4 Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	На посадах наукових і науково-педагогічних працівників в наукових установах і закладах вищої освіти; працівників найвищої кваліфікації у науково-дослідницьких та проектно-конструкторських підрозділах підприємств. Види економічної діяльності за класифікатором ДК 009:2010: Секція М, розділ 72 «Наукові дослідження та розробки»; Секція Р, розділ 85 «Освіта»,

	група 85.4 «Вища освіта», клас 85.42 «Вища освіта»; Секція J, розділ 62 «Комп'ютерне програмування, консультування та пов'язана з ними діяльність» та розділ 63 «Надання інформаційних послуг». Посади згідно класифікатору професій України: 2131.1 Наукові співробітники (обчислювальні системи) 2132.2 Конструктор систем кібербезпеки 2139.1 Наукові співробітники (інші галузі обчислень) 2139.2 Аналітик загроз безпеки, Аналітик з безпеки інформаційно-комунікаційних систем, Аналітик з оцінки вразливостей, Аналітик систем захисту інформації, Аудитор інформаційних технологій (з кібербезпеки), Фахівець з кібердосліджень та розробок систем безпеки 2149.2 Професіонал із організації захисту інформації з обмеженим доступом 2310 Викладачі закладів вищої освіти 2359 Інші професіонали в галузі освіти та навчання 2359.2 Інструктор-методист з інформаційної безпеки та кібербезпеки 2447.1 Наукові співробітники (проекти та програми)
Подальше навчання	Доктор філософії може проводити наукові дослідження в науковій та професійній сферах діяльності, а також інших споріднених галузях наукових знань: – здобуття наукового ступеня доктора наук; – освітні програми, дослідницькі гранти та стипендії (у тому числі й за кордоном).
1.5 Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, самостійна науково-навчальна робота на основі науково-технічної навчальної літератури та публікацій у фахових періодичних виданнях, консультування із науковим керівником, науково-педагогічною спільнотою, проведення наукового дослідження, підготовка та захист дисертаційної роботи.
Оцінювання	Оцінювання навчальних досягнень аспірантів здійснюється за рейтинговою шкалою (прохідні бали 60…100) та за інституційною шкалою («відмінно», «добре», «задовільно», «незадовільно»). Оцінювання включає весь спектр контрольних процедур у залежності від компетентністних характеристик (знання, уміння/навички, комунікація, автономія і відповідальність) результатів навчання, досягнення яких контролюється. Результати навчання аспірантів, що відображають досягнутий ним рівень компетентностей відносно очікуваних, ідентифікуються та вимірюються під час контрольних заходів за допомогою критеріїв, що корелюються з вимогами Національної рамки кваліфікацій і характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою.
Форма випускної атестації	Підсумкова атестація здійснюється у формі публічного захисту дисертаційної роботи доктора філософії. Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв’язання комплексної проблеми в сфері кібербезпеки та захисту інформації та/або на її межі з дотичними спеціальностями, результати якого мають наукову новизну, теоретичне та практичне значення. Дисертація не повинна містити академічного плагіату, фальсифікації, фабрикації. Дисертація має бути розміщена на сайті закладу вищої освіти (наукової установи).
1.6 Ресурсне забезпечення реалізації програми	
Специфічні	Кадрове забезпечення відповідає кадровим вимогам щодо забезпечення

характеристики кадрового забезпечення	провадження освітньої діяльності для третього рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності. До проведення аудиторних занять залучаються професіонали-практики з Придніпровського центру технічного захисту інформації. За необхідності залучаються наукові та науково-педагогічні працівники з інших ЗВО України, з якими укладені відповідні договори про співпрацю. Викладачі періодично посилюють свою підготовку через процедуру підвищення кваліфікації.
Специфічні характеристики матеріально-технічного забезпечення	Матеріально-технічне забезпечення відповідає технологічним вимогам щодо забезпечення провадження освітньої діяльності для третього рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності. Підготовка за даною освітньою програмою здійснюється в лабораторіях: електроніки; комп'ютерного моделювання; засобів технічного захисту інформації; кібербезпеки, - із використанням комплексів засобів захисту «Гриф», автоматизованого комплексу радіомоніторингу "АКОР-2ПК-М", багатофункціональних пошукових пристроїв ST-031P „Піранья" та СРМ-700 «Акула».
Специфічні характеристики інформаційного та навчально-методичного забезпечення	Навчально-методичні матеріали розміщено у хмарних сховищах Microsoft Teams, а також у електронній системі дистанційного навчання Moodle: https://do.nmu.org.ua/
1.7 Академічна мобільність	
Національна кредитна мобільність	Можливість академічної мобільності у ЗВО-партнерах шляхом стажування, навчання, виконання досліджень.
Міжнародна кредитна мобільність	Можлива, але не є обов'язковою. Процедура відбору на програми академічної мобільності: https://projects.nmu.org.ua/ua/Selection procedure applied for the selection of students and staff for mobility.pdf
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти не передбачено.

2. ОБОВ'ЯЗКОВІ КОМПЕТЕНТНОСТІ

Інтегральна компетентність доктора філософії зі спеціальності 125 Кібербезпека та захист інформації – здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації та в дотичних до неї міждисциплінарних напрямах, застосовувати методологію наукової та педагогічної діяльності, проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

2.1 Загальні компетентності

Шифр	Компетентності
ЗК01	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК02	Здатність розв’язувати комплексні проблеми у сфері кібербезпеки та захисту інформації та в дотичних до неї міждисциплінарних напрямах на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.
ЗК03	Здатність працювати в міжнародному контексті.
ЗК04	Здатність презентувати ідеї, інноваційні розробки і результати досліджень як в науковій так і в професійній спільноті.

2.2 Спеціальні (фахові, предметні) компетентності

Шифр	Компетентності
СК01	Здатність інтегрувати знання з різних галузей, застосовувати системний підхід та враховувати нетехнічні аспекти при розв’язанні комплексних проблем кібербезпеки та захисту інформації й проведенні досліджень.
СК02	Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері кібербезпеки та захисту інформації, оцінювати та забезпечувати якість виконуваних досліджень.
СК03	Здатність отримувати нові наукові результати, які створюють нові знання та становлять оригінальний внесок у розвиток кібербезпеки та захисту інформації та дотичних до неї міждисциплінарних напрямів.
СК04	Здатність відстежувати тенденції розвитку кібербезпеки та захисту інформації та критично переосмислювати наявні технології.
СК05	Здатність до розроблення нових та вдосконалення існуючих моделей, методів, засобів, процесів у сфері кібербезпеки та захисту інформації, які забезпечують розвиток або надають нові можливості технологіям розробки та супроводження систем кібербезпеки та захисту інформації.
СК06	Здатність до застосування сучасних методологій, методів та інструментів кібербезпеки та захисту інформації в науково-педагогічній та науковій діяльності.
СК07	Здатність ініціювати, розробляти та реалізовувати дослідницькі та інноваційні проєкти у сфері кібербезпеки та захисту інформації, планувати й організовувати роботу дослідницьких колективів.
СК08	Здатність здійснювати та організовувати науковопедагогічну діяльність у закладах вищої освіти.
Спеціальні компетентності з урахуванням особливостей освітньої програми	
СК09	Здатність до планування та реалізації комплексної інноваційно-пошукової та науково-дослідної діяльності із розробки методів, моделей та засобів безпеки кіберфізичних систем.

3. НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ДОКТОРА ФІЛОСОФІЇ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Результати навчання доктора філософії зі спеціальності 125 Кібербезпека та захист інформації, що визначають нормативний зміст підготовки і корелюються з переліком загальних і спеціальних компетентностей, подано нижче.

Шифр	Результати навчання

Шифр	Результати навчання
РН01	Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації та дотичних до неї міждисциплінарних напрямів, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.
РН02	Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм академічної і професійної етики, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.
РН03	Пропонувати нові ефективні методи і моделі розроблення, впровадження, супроводу та забезпечення якості захищених кіберфізичних систем на всіх етапах життєвого циклу.
РН04	Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях.
РН05	Застосовувати сучасні процедури, інструменти і технології ідентифікації, захисту, виявлення, реагування та відновлення кіберфізичних систем для забезпечення сталого кіберзахисту.
РН06	Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.
РН07	Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах.
РН08	Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосовувати їх у власних дослідженнях та у викладацькій практиці.
РН09	Формулювати та вирішувати задачі оптимізації, адаптації, прогнозування, керування та прийняття рішень щодо процесів, методів і засобів кібербезпеки та захисту інформації.
РН10	Аналізувати та оцінювати стан і перспективи розвитку кібербезпеки та захисту інформації та інформаційних технологій у цілому.
РН11	Розробляти та реалізовувати наукові та/або інноваційні проєкти, які дають змогу переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та прикладні проблеми кібербезпеки та захисту інформації з дотриманням норм академічної етики і врахуванням соціальних, економічних та правових аспектів.
РН12	Забезпечувати захист інтелектуальної власності у сфері кібербезпеки та захисту інформації.
РН13	Організовувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.
	Спеціальні результати навчання з урахуванням особливостей освітньої програми
РН14	Планувати та реалізовувати комплексну інноваційно-пошукову та науково-дослідну діяльність із розробки моделей та засобів криптографічного та технічного захисту в кіберфізичних системах із урахуванням вимог до кіберстійкості.

4. РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр РН	Результати навчання	Найменування освітніх компонентів
1 ОБОВ'ЯЗКОВА ЧАСТИНА		
РН01	Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації та дотичних до неї міждисциплінарних напрямів, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.	Методологія наукових досліджень Інтелектуальні системи в кібербезпеці Криптологія кіберфізичних систем Методи і засоби забезпечення кіберстійкості систем
РН02	Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм академічної і професійної етики, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.	Філософія науки та професійна етика Методологія наукових досліджень Криптологія кіберфізичних систем.
РН03	Пропонувати нові ефективні методи і моделі розроблення, впровадження, супроводу та забезпечення якості захищених кіберфізичних систем на всіх етапах життєвого циклу.	Інтелектуальні системи в кібербезпеці Методи і засоби забезпечення кіберстійкості систем
РН04	Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях.	Іноземна мова для науки і освіти (англійська/німецька/французька)
РН05	Застосовувати сучасні процедури, інструменти і технології ідентифікації, захисту, виявлення, реагування та відновлення кіберфізичних систем для забезпечення сталого кіберзахисту.	Інтелектуальні системи в кібербезпеці Криптологія кіберфізичних систем Методи і засоби забезпечення кіберстійкості систем
РН06	Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема,	Інтелектуальні системи в кібербезпеці

Шифр РН	Результати навчання	Найменування освітніх компонентів
	результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.	
РН07	Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах.	Інтелектуальні системи в кібербезпеці
РН08	Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосовувати їх у власних дослідженнях та у викладацькій практиці.	Методологія наукових досліджень Педагогічна майстерність та прикладна психологія
РН09	Формулювати та вирішувати задачі оптимізації, адаптації, прогнозування, керування та прийняття рішень щодо процесів, методів і засобів кібербезпеки та захисту інформації.	Криптологія кіберфізичних систем Інтелектуальні системи в кібербезпеці Методи і засоби забезпечення кіберстійкості систем
РН10	Аналізувати та оцінювати стан і перспективи розвитку кібербезпеки та захисту інформації та інформаційних технологій у цілому.	Сучасні інформаційні технології у науковій діяльності та управління проектами Методи і засоби забезпечення кіберстійкості систем
РН11	Розробляти та реалізовувати наукові та/або інноваційні проєкти, які дають змогу переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та прикладні проблеми кібербезпеки та захисту інформації з дотриманням норм академічної етики і врахуванням соціальних, економічних та правових аспектів.	Філософія науки та професійна етика Сучасні інформаційні технології у науковій діяльності та управління проектами
РН12	Забезпечувати захист інтелектуальної власності у сфері кібербезпеки та захисту інформації.	Методологія наукових досліджень
РН13	Організовувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.	Педагогічна майстерність та прикладна психологія Викладацька практика

Шифр РН	Результати навчання	Найменування освітніх компонентів
РН14	Планувати та реалізовувати комплексну інноваційно-пошукову та науково-дослідну діяльність із розробки моделей та засобів криптографічного та технічного захисту в кіберфізичних системах із урахуванням вимог до кіберстійкості.	Інтелектуальні системи в кібербезпеці Криптологія кіберфізичних систем Методи і засоби забезпечення кіберстійкості систем
2 ВИБІРКОВА ЧАСТИНА **Визначається завдяки вибору аспірантами навчальних дисциплін із запропонованого переліку**		

5. РОЗПОДІЛ ОБСЯГУ ПРОГРАМИ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр	Освітній компонент	Обсяг, кред.	Підсум. контр.	Розподіл за чвертями
1	*2*	*3*	*4*	*6*
1	**ОБОВ'ЯЗКОВА ЧАСТИНА**	**40**		
1.1	**Цикл загальної підготовки**	**10**		
З1	Філософія науки та професійна етика	4	дз	3;4
З2	Іноземна мова для науки і освіти (англійська/німецька/французька)	6	іс	1;2;3;4
1.2	**Цикл спеціальної підготовки**	**30**		
	Базові дисципліни			
Б1	Методологія наукових досліджень	3	дз	3
Б2	Педагогічна майстерність та прикладна психологія	3	дз	4
Б3	Сучасні інформаційні технології у науковій діяльності та управління проектами	3	дз	1;2
1.2.2	*Фахові освітні компоненти за спеціальністю*			
Ф1	Інтелектуальні системи в кібербезпеці	6	іс	1;2;3;4
Ф2	Криптологія кіберфізичних систем	6	іс	5;6
Ф3	Методи і засоби забезпечення кіберстійкості систем	6	іс	5;6
	Практична підготовка за спеціальністю			
П1	Викладацька практика	3	дз	8
2	**ВИБІРКОВА ЧАСТИНА** **Визначається завдяки вибору аспірантами навчальних дисциплін із запропонованого переліку**	**20**		
	Разом за обов'язковою та вибірковою частинами	**60**		

6. СТРУКТУРНО-ЛОГІЧНА СХЕМА

Послідовність навчальної діяльності аспіранта за денною формою навчання (обов'язкова частина) подана нижче.

Курс	Семестр	Чверть	Шифри освітніх компонентів	Річний обсяг, кредити	Кількість освітніх компонент, що викладаються протягом		
					чверті	семестру	навчального року
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	1	1	З2;Б3;Ф1	25	3	3	6
		2	З2;Б3;Ф1		3		
	2	3	З1;З2;Б1;Ф1		4	5	
		4	З1;З2;Б2;Ф1		4		
2	3	5	Ф2, Ф3	35	2	2	3
		6	Ф2, Ф3		2		
	4	7	(В)			1	
		8	П1		1		

Примітка: Кількість кредитів ЄКТС вказано з урахуванням вибіркових дисциплін. Фактична кількість освітніх компонентів у чвертях та семестрах з урахуванням вибіркових навчальних дисциплін (В) визначається після обрання навчальних дисциплін здобувачами вищої освіти.

7. МАТРИЦІ ВІДПОВІДНОСТІ

Таблиця 1. Матриця відповідності визначених освітньою програмою компетентностей компонентам освітньої програми

		Компоненти освітньої програми								
		З1	З2	Б1	Б2	Б3	Ф1	Ф2	Ф3	П1
Компетентності	ЗК01		*	*						
	ЗК02	*			*					*
	ЗК03		*			*				
	ЗК04	*	*		*					*
	СК01			*			*		*	
	СК02			*				*		
	СК03			*			*			
	СК04					*		*	*	
	СК05						*	*	*	
	СК06				*	*				*
	СК07				*	*				
	СК08				*					*
	СК09						*	*	*	

Таблиця 2. Матриця відповідності результатів навчання компонентам освітньої програми

		Компоненти освітньої програми								
		З1	З2	Б1	Б2	Б3	Ф1	Ф2	Ф3	П1
Результати навчання	РН01			*			*	*	*	
	РН02	*		*				*		
	РН03						*		*	
	РН04		*							
	РН05						*	*	*	
	РН06						*			
	РН07						*			
	РН08			*	*					
	РН09						*	*	*	
	РН10					*			*	
	РН11	*				*				
	РН12			*						
	РН13				*					*
	РН14						*	*	*	

8. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Програма розроблена з урахуванням нормативних та інструктивних матеріалів міжнародного, галузевого та державного рівнів:

1. Закон України «Про вищу освіту» [Електронний ресурс].- Режим доступу: https://zakon.rada.gov.ua/laws/show/1556-18.

2. Закон України «Про освіту» [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2145-19.

3. Національна рамка кваліфікацій (в редакції постанови кабінету Міністрів України від 25 червня 2020р. №519). [Електронний ресурс]. - режим доступу: https://zakon.rada.gov.ua/laws/show/519-2020-%D0%BF#Text.

4. Методичні рекомендації щодо розроблення стандартів вищої освіти. Наказ МОНУ від 01.06.2016 № 600 (у редакції наказу МОНУ від 30.04.2020 № 584).

5. Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти, затверджене Наказом Міністерства освіти і науки України від 11 липня 2019 р. № 977. Зареєстровано в Міністерстві юстиції України 08 серпня 2019 р. за № 880/33851. [Електронний ресурс]. https://zakon.rada.gov.ua/laws/show/z0880-19.

6. Критерії оцінювання якості освітньої програми. Додаток до Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти (пункт 6 розділу І). [Електронний ресурс]. https://naqa.gov.ua/wp-content/uploads/2019/09/Критерії.pdf.

7. Квіт Сергій. Дорожня карта реформування вищої освіти України. Освітня політика. Портал громадських експертів. [Електронний ресурс]. http://education-ua.org/ua/articles/1159-dorozhnya-karta-reformuvannya-vishchoji-osviti-ukrajini.

8. Глосарій. Національне агентство із забезпечення якості вищої освіти. [Електронний ресурс]. https://naqa.gov.ua/wp-content/uploads/2020/01/%d0%93%d0%bb%d0%be%d1%81%d0%b0%d1%80%d1%96%d0%b9.pdf.

9. Довідник користувача ЄКТС [Електронний ресурс]. http://mdu.in.ua/Ucheb/dovidnik_koristuvacha_ekts.pdf.

10. Лист Міністерства освіти і науки України від 28.04.2017 р. №1/9–239 щодо використання у роботі закладів вищої освіти примірних зразків освітніх програм.

11. Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження ліцензійних умов провадження освітньої діяльності» (в редакції постанови КМУ від 24 березня 2021 р. № 365).

12. Лист Міністерства освіти і науки України від 05.06.2018 р. №1/9–377 щодо надання роз'яснень стосовно освітніх програм.

13. Положення про організацію освітнього процесу Національного технічного університету «Дніпровська політехніка». https://www.nmu.org.ua/ua/content/activity/us_documents/Pologenie_pro_organiz_osvit_process_2019.pdf

14. Положення про систему запобігання та виявлення плагіату Національного

технічного університету «Дніпровська політехніка». https://www.nmu.org.ua/ua/content/activity/us_documents.pdf

15. Положення про формування переліку та обрання навчальних дисциплін здобувачами вищої освіти Національного технічного університету «Дніпровська політехніка». https://www.nmu.org.ua/ua/content/activity/us_documents_2021.pdf

16. Положення про викладацьку практику здобувачів вищої освіти ступеня доктора філософії Національного технічного університету «Дніпровська політехніка». Затверджено Вченою радою університету від 27.04.2020, протокол № 4. [Електронний ресурс]. https://cutt.ly/OZEfnCU.

17.Положення про підготовку здобувачів вищої освіти ступеня доктора філософії та доктора наук у Національному технічному університеті «Дніпровська політехніка». Затверджено Вченою радою університету від 18.09.2018, протокол № 11. [Електронний ресурс]. https://cutt.ly/kZEfDUA.

Освітня програма оприлюднюється на сайті університету до початку прийому здобувачів на навчання.

Освітня програма поширюється на всі кафедри університету та вводиться в дію з 1-го жовтня 2024 року.

Освітня програма підлягає перегляду та доопрацюванню відповідно до змін нормативної бази України в сфері вищої освіти.

Відповідальність за впровадження освітньої програми та забезпечення якості вищої освіти несе гарант освітньої програми.

Навчальне видання

Корченко Анна Олександрівна
Іванченко Олег Васильович
Котух Євген Володимирович
Давиденко Кирило Олександрович

ОСВІТНЬО-НАУКОВА ПРОГРАМА ДОКТОРА ФІЛОСОФІЇ «БЕЗПЕКА КІБЕРФІЗИЧНИХ СИСТЕМ» ЗА СПЕЦІАЛЬНІСТЮ 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Електронний ресурс

Видано
у Національному технічному університеті
«Дніпровська політехніка».
Свідоцтво про внесення до Державного реєстру ДК № 1842 від 11.06.2004.
49005, м. Дніпро, просп. Дмитра Яворницького, 19.

РЕЦЕНЗІЯ СТЕЙКХОЛДЕРА

на освітньо-наукову програму «Безпека кіберфізичних систем» підготовки здобувачів освіти третього (освітньо-наукового) рівня підготовки у галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації»

Швидка еволюція ІТ-галузі вимагає розвинутої системи захисту інформації та реагування на запити ринку праці, зокрема, враховуючи галузевий та регіональний контекст. У місті Дніпро протягом останніх років спостерігається стійкий розвиток ІТ-галузі, який продукує потребу у фахівцях з кібербезпеки та захисту інформації. В той же час, на ринку праці регіону спостерігається стійкий дефіцит кваліфікованих кадрів, зокрема професіоналів високого рівня, що володіють знаннями у галузі інформаційних технологій, здатних розв'язувати складні наукові та практичні проблеми забезпечення захищеності інформації в інформаційно-комунікаційних системах, що дозволить випускникам успішно здійснювати дослідження, проектування, впровадження, експлуатацію та модернізацію сучасних систем та технологій інформаційної та/або кібербезпеки.

Розроблена освітньо-наукова програма «Безпека кіберфізичних систем» для докторів філософії за спеціальністю 125 Кібербезпека та захист інформації відповідає сучасним вимогам до підготовки фахівців, здатних забезпечити на території області та всієї України реалізацію державної політики у сфері цифрового розвитку, цифрових трансформацій і цифровізації.

Особливостями програми є її спрямованість на вивчення перспективних напрямків розробок інтелектуальних методів, забезпечення глибоких знань щодо сучасних засобів захисту інформації. ОНП орієнтована на інновації систем та технологій кібербезпеки і забезпечення захищеності інформації, що обробляється (передається) в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, зокрема, критичної інформаційної інфраструктури.

Зміст освітньо-професійної програми, реалізації її компетентністного підходу, логічна упорядкованість освітніх компонентів надають можливість послідовно досягнути зазначених компетентностей і програмних результатів навчання та створюють усі умови для всебічного розвитку особистості здобувача.

З огляду на вищезазначене, вважаю, що рецензована Освітньо-наукова програма «Безпека кіберфізичних систем» спеціальності 125 «Кібербезпека та захист інформації» є збалансованою, актуальною та такою, що відповідає сучасним вимогам, а тому рекомендується до затвердження для підготовки здобувачів третього (освітньо-наукового) рівня у галузі знань 12 «Інформаційні технології».

Директор департаменту цифрової трансформації, інформаційних технологій та електронного урядування Дніпропетровської обласної державної адміністрації — Євген ДОН

РЕЦЕНЗІЯ

на освітньо-наукову програму «Безпека кіберфізичних систем» підготовки здобувачів освіти третього (освітньо-наукового) рівня підготовки у галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації»

Освітньо-наукова програма, що підготовлена кафедрою безпеки інформації та телекомунікацій і реалізується в Національному технічному університеті «Дніпровська політехніка», враховує сучасні тенденції розвитку ІТ-галузі і вимог ринку праці.

Програма містить перспективні напрямки розробок штучного інтелекту, забезпечує глибокі знання щодо сучасних моделей, методів, алгоритмів інтелектуального аналізу та захисту інформації, технологій Big Data, веб-технологій, передбачає вивчення сучасних засобів інформаційно-комунікаційних технологій.

Перелік компетентностей здобувача, логічна упорядкованість та актуальність визначених освітньо-науковою програмою освітніх компонентів, їх відповідність вимогам та запитам сучасного ринку праці з ІТ-галузі не викликають сумніву. Кінцеві, підсумкові та інтегративні результати навчання здобувача ступеня доктора філософія зі спеціальності 125 Кібербезпека та захист інформації відповідають сучасним вимогам до підготовки фахівців, здатних розв'язувати складні наукові та практичні проблеми забезпечення захищеності інформації, яка обробляється (передається) в інформаційно-комунікаційних системах, що дозволить випускникам успішно здійснювати дослідження, проектування, впровадження, експлуатацію та модернізацію сучасних систем та технологій інформаційної та/або кібербезпеки на принципах академічної доброчесності, загальнолюдських цінностей, національної ідентичності та креативного становлення людини і суспільства майбутнього. Позитивним аспектом є можливість формування індивідуальної освітньої траєкторії через вільний вибір освітніх компонентів з вибіркового блоку.

У рецензованій програмі обґрунтовано визначені об'єкт і цілі навчання, теоретичний зміст предметної області, методи і методики навчання та наукових досліджень.

На основі вищезазначеного вважаю, що освітньо-наукова програма "Безпека кіберфізичних систем" є актуальною, відповідає сучасним тенденціям розвитку інформаційних технологій і вимогам ринку праці та може бути рекомендована для підготовки фахівців із захисту інформації.

Начальник сектору захисту критичної інфраструктури Управління Держспецзв'язку у Дніпропетровській області, підполковник Юрій ПОНОМАРЕНКО