ПРОЄКТ

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

ЗАТВЕРДЖЕНО
Вченою радою університету
____червня 2026 р., протокол № __

Голова Вченої ради
_____Генанадій ПІВНЯК

ОСВІТНЬО-НАУКОВА ПРОГРАМА ВИЩОЇ ОСВІТИ
«Безпека кіберфізичних систем»

ГАЛУЗЬ ЗНАНЬ	F Інформаційні технології
СПЕЦІАЛЬНІСТЬ	F5 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 _01.10.2026р.

Наказ від ___ червня 2026р., № __

Ректор

_____Олександр АЗЮКОВСЬКИЙ

Дніпро
НТУ «ДП»
2026

ЛИСТ-ПОГОДЖЕННЯ

Центр моніторингу знань та тестування
протокол № _____ від «__»_____2026 р.

Директор _____ _____
(підпис, ініціали, прізвище)

Відділ внутрішнього забезпечення якості вищої освіти
протокол № _____ від «__»_____2026 р.

Начальник відділу _____ _____
(підпис, ініціали, прізвище)

Навчально-методичний відділ
протокол №_____ від «__»_____2026 р.

Начальник відділу _____ _Ю.О. Заболотна_
(підпис, ініціали, прізвище)

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

Науково-методична комісія спеціальності F5 Кібербезпека та захист інформації

Протокол № ____ від «__» _____ 2026 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.
2.

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) та стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації для для третього (освітньо-наукового) рівня (наказ МОН від 29.10.2024 № 1543).

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 F5 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 F5 Кібербезпека та захист інформації;

Дія освітньої програми поширюється на кафедри університету, що беруть участь у підготовці фахівців ступеня доктора філософії спеціальності F5 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	F Інформаційні технології / F5 Кібербезпека та захист інформації *Об'єкти вивчення та діяльності:* – інформаційні системи і технології 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, концепції, теорії захисту життєво важливих інтересів людини і громадянина, суспільства та 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:* сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, методи статистичного аналізу даних. *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).
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 в кіберфізичних системах на об'єктах інформаційної діяльності та критичної інфраструктури, 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 M, розділ 72 «Наукові дослідження та розробки»; Секція P, 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 характеристики кадрового забезпечення	Кадрове забезпечення відповідає кадровим вимогам щодо 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 F5 Кібербезпека та захист інформації – здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

2.1 Загальні компетентності

Шифр	Компетентності
ЗК1	Здатність до абстрактного мислення, аналізу і синтезу.
ЗК2	Здатність до пошуку, оброблення, та аналізу інформації з різних джерел.
ЗК3	Здатність працювати в міжнародному контексті.
ЗК4	Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із

	дотриманням принципів професійної етики та академічної доброчесності.

2.2 Спеціальні (фахові, предметні) компетентності

Шифр	Компетентності
СК1	Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації.
СК2	Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації.
СК3	Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики.
СК4	Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації.
СК5	Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень.
СК6	Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому українською та англійською мовами.
СК7	Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти.
Спеціальні компетентності з урахуванням особливостей освітньої програми	
СК8	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
РН1	Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій.
РН2	Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики.
РН3	Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.

Шифр	Результати навчання
РН4	Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосовувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці.
РН5	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.
РН6	Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних вітчизняних та міжнародних наукових виданнях.
РН7	Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації.
РН8	Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах.
РН9	Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.
РН10	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
РН11	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		
РН1	Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій.	Методологія наукових досліджень Інтелектуальні системи в кібербезпеці Криптологія кіберфізичних систем Методи і засоби забезпечення кіберстійкості систем
РН2	Планувати і виконувати експериментальні та/або теоретичні	Філософія науки та професійна етика Методологія наукових досліджень

Шифр РН	Результати навчання	Найменування освітніх компонентів
	дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики.	Криптологія кіберфізичних систем.
РН3	Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.	Методологія наукових досліджень Сучасні інформаційні технології у науковій діяльності та управління проектами
РН4	Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосовувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці.	Методологія наукових досліджень Педагогічна майстерність та прикладна психологія
РН5	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.	Інтелектуальні системи в кібербезпеці Методи і засоби забезпечення кіберстійкості систем
РН6	Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних вітчизняних та міжнародних наукових виданнях.	Іноземна мова для науки і освіти (англійська/німецька/французька) Педагогічна майстерність та прикладна психологія
РН7	Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації.	Інтелектуальні системи в кібербезпеці Криптологія кіберфізичних систем Методи і засоби забезпечення кіберстійкості систем
РН8	Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у	Інтелектуальні системи в кібербезпеці Методи і засоби забезпечення кіберстійкості систем

Шифр РН	Результати навчання	Найменування освітніх компонентів
	кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах.	
РН9	Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.	Сучасні інформаційні технології у науковій діяльності та управління проектами Інтелектуальні системи в кібербезпеці
РН10	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
РН11	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	ЗК1		*	*						
	ЗК2	*			*					*
	ЗК3		*			*				
	ЗК4	*	*		*					*
	СК1			*			*		*	
	СК2			*				*		
	СК3			*			*			
	СК4					*		*	*	
	СК5						*	*	*	
	СК6				*	*				*
	СК7				*	*				
	СК8						*	*	*	

Таблиця 2. Матриця відповідності результатів навчання компонентам освітньої програми

		Компоненти освітньої програми								
		З1	З2	Б1	Б2	Б3	Ф1	Ф2	Ф3	П1
Результати навчання	РН1			*			*	*	*	
	РН2	*		*				*		
	РН3			*		*				
	РН4			*	*					
	РН5						*		*	
	РН6		*		*					
	РН7						*	*	*	
	РН8						*		*	
	РН9					*	*			
	РН10				*					*
	РН11						*	*	*	

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.

18.Стандарт вищої освіти підготовки доктора філософії зі спеціальності 125 Кібербезпека та захист інформації. СВО-2024. – К. : МОН України, 2024. – 14 с. – Затверджено і введено в дію наказом МОН України від 29.10.2024 р. № 1543.

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 2026 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 F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ**

Електронний ресурс

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