

ПРОЄКТ 2021

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

ЗАТВЕРДЖЕНО
Вченою радою університету

Голова Вченої ради

_____ Г.Г. Півняк
«__» _____ 2021 р.,
протокол № _____

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ВИЩОЇ ОСВІТИ
«Кібербезпека»

ГАЛУЗЬ ЗНАНЬ	12 Інформаційні технології
СПЕЦІАЛЬНІСТЬ	125 Кібербезпека
РІВЕНЬ ВИЩОЇ ОСВІТИ	Другий (магістерський)
СТУПІНЬ	Магістр
ОСВІТНЯ КВАЛІФІКАЦІЯ	Магістр з кібербезпеки

Уводиться в дію з 01.09.2021

Ректор

_____ Г.Г. Півняк

Наказ від

№ _____

Дніпро
НТУ «ДП»
2021

ЛИСТ-ПОГОДЖЕННЯ

Центр моніторингу знань та тестування
протокол № _____ від «__» _____ 20__ р.

Директор _____
(підпис) (ініціали, прізвище)

Сектор ліцензування та акредитації навчально-методичного відділу
протокол № _____ від «__» _____ 20__ р.

Керівник сектору _____
(підпис) (ініціали, прізвище)

Відділ внутрішнього забезпечення якості вищої освіти
протокол № _____ від «__» _____ 20__ р.

Начальник відділу _____
(підпис) (ініціали, прізвище)

Навчально-методичний відділ
протокол № _____ від «__» _____ 20__ р.

Начальник відділу _____
(підпис) (ініціали, прізвище)

Науково-методична комісія спеціальності 125 Кібербезпека
Протокол № _____ від «__» _____ 20__ р.

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

Гарант освітньої програми _____ В.І. Корнієнко.
(підпис) (ініціали, прізвище)

Кафедра безпеки інформації та телекомунікацій
Протокол № _____ від «__» _____ 20__ р.

Завідувач кафедри _____ В.І. Корнієнко
(підпис) (ініціали, прізвище)

Декан факультету
інформаційних технологій _____ М.О. Алексєєв
(підпис) (ініціали, прізвище)

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Корнієнко Валерій Іванович, д.т.н., професор, завідувач кафедри безпеки інформації та телекомунікацій.
2. Герасіна Олександра Володимирівна, к.т.н., доцент, доцент кафедри безпеки інформації та телекомунікацій.
3. Кагадій Тетяна Станіславівна, д.ф.-м.н., професор, професор кафедри безпеки інформації та телекомунікацій.
4. Кручинін Олександр Володимирович, старший викладач кафедри безпеки інформації та телекомунікацій.
5. Тимофєєв Дмитро Сергійович, старший викладач кафедри безпеки інформації та телекомунікацій.

ЗМІСТ

ВСТУП	5
1 ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ	5
2 ОБОВ'ЯЗКОВІ КОМПЕТЕНТНОСТІ	9
3 НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ	10
4 РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ	11
5 РОЗПОДІЛ ОБСЯГУ ПРОГРАМИ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ	13
6 СТРУКТУРНО-ЛОГІЧНА СХЕМА	14
7 МАТРИЦІ ВІДПОВІДНОСТІ	15
8 ПРИКІНЦЕВІ ПОЛОЖЕННЯ	17
ДОДАТКИ	19

ВСТУП

Освітньо-професійна програма розроблена на основі проєкту Стандарту вищої освіти підготовки магістрів спеціальності 125 Кібербезпека.

Освітньо-професійна програма використовується під час:

- ліцензування спеціальності та акредитації освітньої програми;
- складання навчальних планів;
- формування робочих програм навчальних дисциплін, силабусів, програм практик, індивідуальних завдань;
- формування індивідуальних навчальних планів студентів;
- розроблення засобів діагностики якості вищої освіти;
- атестації магістрів спеціальності 125 Кібербезпека;
- визначення змісту навчання в системі перепідготовки та підвищення кваліфікації;
- професійної орієнтації здобувачів фаху;
- зовнішнього контролю якості підготовки фахівців.

Користувачі освітньо-професійної програми:

- здобувачі вищої освіти, які навчаються в НТУ «ДП»;
- викладачі НТУ «ДП», які здійснюють підготовку магістрів спеціальності 125 «Кібербезпека»;
- екзаменаційна комісія спеціальності 125 Кібербезпека;
- приймальна комісія НТУ «ДП».

Освітньо-професійна програма поширюється на кафедри університету, які беруть участь у підготовці фахівців ступеня магістр спеціальності 125 Кібербезпека.

1 ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

1.1 Загальна інформація	
Повна назва закладу вищої освіти та інститут (факультет)	Національний технічний університет «Дніпровська політехніка», факультет інформаційних технологій, кафедра безпеки інформації та телекомунікацій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом магістра, 90 кредитів ЄКТС, термін навчання – 1 рік 4 місяці
Наявність акредитації	Міністерство освіти і науки України, Україна. Сертифікат про акредитацію спеціальності УД 04002581 відповідно до рішення Акредитаційної комісії від 2 березня 2017 р. протокол №124 (наказ МОН України від 13.03.2017 р. №375, на підставі наказу МОН України від 19.12.2016 №1565) Строк дії сертифіката до 01 липня 2022 р.

	Акредитація освітньої програми не проводилася
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Особа має право здобувати ступінь магістра за умови наявності в неї першого (бакалаврського) рівня вищої освіти зі спеціальності 125 Кібербезпека або іншої спорідненої спеціальності Особливості вступу на освітню програму 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 1 рік 4 місяці та/або період акредитації. Освітня програма підлягає перегляду відповідно до змін нормативної бази України в сфері вищої освіти, але не рідше одного разу на рік.
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.bit.nmu.org.ua . Інформаційний пакет за спеціальністю http://www.nmu.org.ua/ua/content/infrastructure/structural_divisions/science_met_dep/educational_programs/ Освітні програми НТУ «ДП»

1.2 Мета освітньої програми

Підготовка фахівців з дослідження та розробки сучасних систем та технологій інформаційної та/або кібербезпеки із забезпеченням органічного поєднання освітньої, наукової та інноваційної діяльності з інтеграцією до міжнародного науково-освітнього простору, яка направлена на здобуття поглиблених теоретичних і практичних знань щодо формування здатності розв'язувати складні наукові та практичні проблеми в області кібербезпеки, що дозволить випускникам освітньої програми успішно здійснювати розробку, впровадження й дослідження у різних галузях людської діяльності, національної економіки та виробництва.

1.3 Характеристика освітньої програми

Предметна область	12 Інформаційні технології / 125 Кібербезпека. Освітня програма: Кібербезпека. Об'єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Цілі навчання: підготовка фахівців з кібербезпеки з формуванням загальних та спеціальних компетентностей, необхідних для інноваційної науково-дослідницької діяльності при дослідженні, проектуванні, модернізації, впровадженні та експлуатації сучасних систем та технологій інформаційної та/або кібербезпеки, інформаційної безпеки інфокомунікаційних систем та мереж. Теоретичний зміст предметної області. Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів розробки та супроводу систем та комплексів інформаційної та/або кібербезпеки;
-------------------	---

	<ul style="list-style-type: none"> – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. <p>Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки.</p> <p>Інструменти та обладнання:</p> <ul style="list-style-type: none"> – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	<p>Освітньо-професійна, прикладна та має наступні професійні (спеціалізаційні) акценти:</p> <ol style="list-style-type: none"> 1. Посилена підготовка в галузі дискретної математики, електроніки, радіотехніки, акустики, дискретної обробки інформації логіко-математичними методами та фізико-технічними засобами; 2. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, яка циркулює на об'єктах інформаційної діяльності державної та приватної форм власності; 3. Посилена підготовка в галузі міждисциплінарного системного аналізу з метою створення комплексних систем захисту інформаційних потоків у комунікаційних мережах; 4. Робочі плани підготовки здобувачів вищої освіти щорічно переглядаються з метою включення розділів, пов'язаних з розвитком знань у галузі кібернетичної безпеки на основі аналізу нових науково-технологічних здобутків; 5. Проведення щорічних конференцій та олімпіад з нових напрямків кібернетичної безпеки з метою навчання здобувачів вищої освіти розробці індивідуальних стартапів на етапі підготовки кваліфікаційної роботи. 6. Формування максимально широкого науково-технічного світогляду майбутнього фахівця.
Основний фокус освітньої програми	<p>Спеціальна освіта в галузі 12 Інформаційні технології / спеціальності 125 Кібербезпека.</p> <p>Підготовка фахівців здатних до інноваційної науково-дослідницької діяльності при дослідженні, проектуванні, модернізації, впровадженні та експлуатації сучасних систем та технологій інформаційної та/або кібербезпеки.</p> <p>Ключові слова: кіберзахист, інформаційна безпека, управління безпекою, інфокомунікаційні системи та мережі</p>
Особливості програми	<p>Виробнича та передатестаційна практика обов'язкові. Проводяться в спеціалізованих комп'ютерних лабораторіях та комп'ютерних класах кафедри, на базі Придніпровського</p>

	регіонального науково-технічного центру технічного захисту інформації а також на підприємствах міста та області. Орієнтованість на інновації систем та технологій інформаційної та кібербезпеки інфокомунікаційних систем та мереж.
1.4 Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Види економічної діяльності за класифікатором видів економічної діяльності ДК 009:2010: Секція J, Розділ 62 Комп'ютерне програмування, консультування та пов'язана з ними діяльність Клас 62.09 Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
Подальше навчання	Можливість навчання за кваліфікаційними рівнями: НРК України – 8, рівень FQ-EHEA – третій цикл, EQF-LLL – 8 рівень
1.5 Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, навчання через лабораторну практику. Лекції, семінари, практичні заняття, лабораторні роботи в малих групах, самостійна робота, консультації із викладачами.
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за рейтинговою шкалою (прохідні бали 60...100) та за інституційною шкалою («відмінно», «добре», «задовільно», «незадовільно»), що використовується для конвертації оцінок мобільних студентів. 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 студента, що відображають досягнутий ним рівень компетентностей відносно очікуваних, ідентифікуються та вимірюються під час контрольних заходів за допомогою критеріїв, що корелюються з описами кваліфікаційних рівнів Національної рамки кваліфікацій і характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою. Підсумковий контроль з навчальних дисциплін здійснюється за результатами поточного контролю або/та оцінюванням виконання комплексної контрольної роботи або/та усних відповідей. Оцінювання результатів проводиться відповідно до Положення університету про оцінювання результатів навчання здобувачів вищої освіти
Форма випускної атестації	Атестація здобувачів вищої освіти здійснюється у формі публічного захисту кваліфікаційної роботи магістра. Кваліфікаційна робота має передбачати розв'язання складної науково-технічної задачі в галузі інформаційної та/або кібербезпеки, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і

	<p>вимог.</p> <p>Робота перевіряється на наявність плагіату згідно з процедурою, визначеною системою забезпечення якості освітньої діяльності та якості вищої освіти університетом.</p> <p>Захист кваліфікаційної роботи відбувається прилюдно на засіданні екзаменаційної комісії.</p> <p>Кваліфікаційна робота оприлюднюється в репозитарії університету</p>
1.6 Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	<p>Кадрове забезпечення відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності для другого (магістерського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності (п.30).</p> <p>До проведення аудиторних занять залучаються професіонали-практики з Придніпровського центру технічного захисту інформації.</p> <p>Викладачі періодично посилюють свою підготовку через процедуру підвищення кваліфікації. Підготовку здобувачів вищої освіти здійснюють 3 професори, 6 доцентів та 2 старших викладачі кафедри безпеки інформації та телекомунікацій із залученням фахівців з інших кафедр.</p>
Специфічні характеристики матеріально-технічного забезпечення	<p>Матеріально-технічне забезпечення відповідає до технологічним вимогам щодо забезпечення провадження освітньої діяльності для другого (магістерського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності.</p> <p>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».</p>
Специфічні характеристики інформаційного та навчально-методичного забезпечення	<p>Інформаційне та навчально-методичне забезпечення відповідає технологічним вимогам щодо навчально-методичного та інформаційного забезпечення провадження освітньої діяльності для другого (магістерського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності.</p> <p>Методичні матеріали розміщені на платформі дистанційної освіти Moodle, сайті кафедри та в додатках сервісів Office 365: https://do.nmu.org.ua/course/index.php?categoryid=5.</p>
1.7 Академічна мобільність	
Національна кредитна мобільність	Можливість укладання угод про академічну мобільність, про подвійне дипломування тощо
Міжнародна кредитна мобільність	<p>Можливість укладання угод про міжнародну мобільність, про подвійне дипломування, про тривалі міжнародні проекти, що передбачають навчання студентів тощо.</p> <p>Положення про академічну мобільність НТУ "Дніпровська політехніка": http://projects.nmu.org.ua/ua/Про затвердження Положення про Мобільність.pdf</p> <p>Стратегія інтернаціоналізації НТУ "Дніпровська політехніка":</p>

	http://projects.nmu.org.ua/ua/Internationalisation_strategy_en_2025.pdf Процедура відбору на програми академічної мобільності: http://projects.nmu.org.ua/ua/Selection_procedure_applied_for_the_selection_of_students_and_staff_for_mobility.pdf Доступні програми мобільності та університети-партнери: 1. Erasmus+ K107: - Університ Хаену, (Іспанія); - Університет Леобену (Австрія); - Чанкири Каратекін Університет (Туреччина); - Вроцлавська політехніка. 2. Стипендія Баден-Вюртемберг (Baden-Wurtemberg): - Університет Еслінгену (програма – Information Technology (B)); - Університет Ройтлінгену, Німеччина. 3. Програма турецьких обмінів Мевлана.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти не передбачено.

2 ОБОВ'ЯЗКОВІ КОМПЕТЕНТНОСТІ

Інтегральна компетентність магістра зі спеціальності 125 Кібербезпека - здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки, що характеризуються комплексністю та неповною визначеністю умов.

2.1 Загальні компетентності

Шифр	Компетентності
1	2
ЗК1	Здатність розв'язувати комплексні задачі та практичні проблеми технологій кібербезпеки в невизначених умовах.
ЗК2	Здатність використовувати методи фундаментальних наук та загально інженерних наук для розв'язання загально інженерних , професійних та наукових задач.
ЗК3	Здатність до ініціативності, відповідальності та навичок до превентивного і аварійного планування, управління заходами безпеки професійної діяльності, уміння приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості на посаді керівника
ЗК4	Здатність до ефективної письмової й усної комунікації українською та іноземною мовами
ЗК5	Здатність працювати в міжнародному контексті та в глобальному інформаційному середовищі за фахом
ЗК6	Здатність до подальшого навчання з високим рівнем автономності.

2.2 Спеціальні компетентності

2.2.1 Спеціальні компетентності

Шифр	Компетентності
------	----------------

1	2
СК1	Здатність використовувати управлінсько-організаційні, математичні, технічні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.
СК2	Здатність проводити системні дослідження та застосовувати їх в керуванні проектами для забезпечення інформаційної та кібербезпеки.
СК3	Здатність використовувати комплексні методи забезпечення інформаційної та кібернетичної безпеки
СК4	Здатність організувати роботу з підвищення науково-технічних знань працівників, організувати розвиток творчої ініціативи, використання передового досвіду.
СК5	Здатність організувати та проводити наукові дослідження, пов'язані із застосуванням математичних та технічних методів для аналізу та дослідження процесів та систем забезпечення інформаційної та кібернетичної безпеки.

2.2.2 Спеціальні компетентності з урахуванням особливостей освітньої програми

Шифр	Компетентності
1	2
СК6	Здатність володіти технологіями розроблення програмних засобів захисту інформації, синтезу комплексів засобів захисту інформації. Здатність до застосування математичного та комп'ютерного моделювання для вирішення широкого спектру задач інформаційної та кібернетичної безпеки.
СК7	Здатність розробляти нові та адаптувати існуючі математичні, комп'ютерні, технічні та фізичні моделі досліджуваних систем та процесів, проводити відповідні експерименти та чисельні розрахунки з аналізом та інтерпретацією отриманих результатів.
СК8	Готовність використовувати сучасні психолого-педагогічні теорії й методи в професійній діяльності. Здатність організувати роботу колективів виконавців, приймати управлінські рішення в умовах спектра думок, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем забезпечення інформаційної та кібернетичної безпеки, систематизувати й узагальнювати результати роботи.
СК9	Здатність до роботи в багатонаціональних колективах, у тому числі при роботі над міждисциплінарними й інноваційними проектами, створювати в колективах відносини ділового співробітництва.
СК10	Здатність готувати та здійснювати публічні виступи з презентацією отриманих результатів, готувати науково – технічні публікації (звіти, статті тощо) за результатами виконаних досліджень.

З НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Кінцеві, підсумкові та інтегративні результати навчання магістра зі спеціальності 125 Кібербезпека, що визначають нормативний зміст підготовки і корелюються з переліком загальних і спеціальних компетентностей, подано нижче.

Шифр	Результати навчання
-------------	----------------------------

<i>1</i>	<i>2</i>
PH1	Розв'язувати комплексні задачі та практичні проблеми технологій кібербезпеки в невизначених умовах.
PH2	Використовувати методи фундаментальних наук та загально інженерних наук для розв'язання загально інженерних , професійних та наукових задач.
PH3	Превентивно і аварійно планувати, управляти заходами безпеки професійної діяльності, приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості на посаді керівника
PH4	Письмова й усна комунікації українською та іноземною мовами
PH5	Співпрацювати в міжнародному контексті та в глобальному інформаційному середовищі за фахом
PH6	Вмотивованість щодо подальшого навчання з високим рівнем автономності.
PH7	Використовувати управлінсько-організаційні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.
PH8	Проводити системні дослідження та застосовувати їх в керуванні проектами для забезпечення інформаційної та кібербезпеки.
PH9	Використовувати математичні, технічні та правові методи забезпечення інформаційної та кібернетичної безпеки
PH10	Організовувати роботи з підвищення науково-технічних знань працівників, організовувати розвиток творчої ініціативи, використання передового досвіду.
PH11	Організовувати та проводити наукові дослідження, пов'язані із застосуванням математичних та технічних методів для аналізу та дослідження процесів та систем забезпечення інформаційної та кібернетичної безпеки.
PH12	Використовувати технології розроблення програмних засобів захисту інформації, синтезу комплексів засобів захисту інформації. Застосовувати математичне та комп'ютерне моделювання для вирішення широкого спектру задач інформаційної та кібернетичної безпеки.
PH13	Розробляти нові та адаптувати існуючі математичні, комп'ютерні, технічні та фізичні моделі досліджуваних систем та процесів, проводити відповідні експерименти та чисельні розрахунки з аналізом та інтерпретацією отриманих результатів.
PH14	Використовувати сучасні психолого-педагогічні теорії й методи в професійній діяльності. Організовувати роботи колективів виконавців, приймати управлінські рішення в умовах спектра думок, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем забезпечення інформаційної та кібернетичної безпеки, систематизація й узагальнення результатів роботи.
PH15	Працювати в багатонаціональних колективах, у тому числі при роботі над міждисциплінарними й інноваційними проектами, створювати в колективах відносини ділового співробітництва.
PH16	Публічно виступати з презентацією отриманих результатів, готувати науково – технічні публікації (звіти, статті тощо) за результатами виконаних досліджень.

4 РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр	Результати навчання	Найменування освітніх компонентів
<i>1</i>	<i>2</i>	<i>3</i>

1	2	3
1 ОБОВ'ЯЗКОВА ЧАСТИНА		
PH1	Розв'язувати комплексні задачі та практичні проблеми технологій кібербезпеки в невизначених умовах.	Технології забезпечення інформаційної і кібербезпеки об'єктів
PH2	Використовувати методи фундаментальних наук та загально інженерних наук для розв'язання загально інженерних , професійних та наукових задач.	Технології забезпечення інформаційної і кібербезпеки об'єктів
PH3	Превентивно і аварійно планувати, управляти заходами безпеки професійної діяльності, приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості на посаді керівника	Управління безпекою, автономність та відповідальність у професійній діяльності
PH4	Письмова й усна комунікації українською та іноземною мовами	Управління безпекою, автономність та відповідальність у професійній діяльності Іноземна мова для професійної діяльності (англ./нім./франц.)
PH5	Співпрацювати в міжнародному контексті та в глобальному інформаційному середовищі за фахом	Іноземна мова для професійної діяльності (англ./нім./франц.)
PH6	Вмотивованість щодо подальшого навчання з високим рівнем автономності.	Управління безпекою, автономність та відповідальність у професійній діяльності
PH7	Використовувати управлінсько-організаційні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.	Технології забезпечення інформаційної і кібербезпеки об'єктів
PH8	Проводити системні дослідження та застосовувати їх в керуванні проектами для забезпечення інформаційної та кібербезпеки.	Технології забезпечення інформаційної і кібербезпеки об'єктів
PH9	Використовувати математичні, технічні та правові методи забезпечення інформаційної та кібернетичної безпеки	Системи управління інформаційною безпекою
PH10	Організовувати роботи з підвищення науково-технічних знань працівників, організовувати розвиток творчої ініціативи, використання передового досвіду.	Управління інноваційними проектами Виробнича практика
PH11	Організовувати та проводити наукові дослідження, пов'язані із застосуванням математичних та технічних методів для аналізу та дослідження процесів та систем забезпечення інформаційної та кібернетичної безпеки.	Виконання кваліфікаційної роботи Передатестаційна практика Виробнича практика
PH12	Використовувати технології розроблення програмних засобів захисту інформації, синтезу комплексів засобів захисту інформації. Застосовувати математичне та комп'ютерне моделювання для вирішення широкого спектру задач інформаційної та кібернетичної безпеки.	Інтелектуальні системи кіберзахисту

1	2	3
PH13	Розробляти нові та адаптувати існуючі математичні, комп'ютерні, технічні та фізичні моделі досліджуваних систем та процесів, проводити відповідні експерименти та чисельні розрахунки з аналізом та інтерпретацією отриманих результатів.	Інтелектуальні системи кіберзахисту Виконання кваліфікаційної роботи
PH14	Використовувати сучасні психолого-педагогічні теорії й методи в професійній діяльності. Організувати роботи колективів виконавців, приймати управлінські рішення в умовах спектра думок, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем забезпечення інформаційної та кібернетичної безпеки, систематизація й узагальнення результатів роботи.	Інтелектуальні системи кіберзахисту Передатестаційна практика
PH15	Працювати в багатонаціональних колективах, у тому числі при роботі над міждисциплінарними й інноваційними проектами, створювати в колективах відносини ділового співробітництва.	Виробнича практика
PH16	Публічно виступати з презентацією отриманих результатів, готувати науково – технічні публікації (звіти, статті тощо) за результатами виконаних досліджень.	Виконання кваліфікаційної роботи

5 РОЗПОДІЛ ОБСЯГУ ПРОГРАМИ ЗА ОСВІТНИМИ КОМПОНЕНТАМИ

Шифр	Освітній компонент	Обсяг, кред.	Підсум. контр.	Кафедра, що викладає	Розподіл за чвертями
1	2	3	4	5	6
1	ОБОВ'ЯЗКОВА ЧАСТИНА	66			
1.1	Цикл загальної підготовки	9			
31	Іноземна мова для професійної діяльності (англійська/ німецька/ французька)	6,0	іс	ІнМов	1;2;3;4
32	Управління безпекою, автономність та відповідальність у професійній діяльності	3,0	дз	ОП та ЦБ	1
1.2	Цикл спеціальної підготовки	57			
1.2.1	<i>Фахові освітні компоненти за спеціальністю</i>	27			
Ф1	Технології забезпечення інформаційної і кібербезпеки об'єктів	8,0	іс	БІТ	1;2
Ф2	Інтелектуальні системи кіберзахисту	10,0	іс	БІТ	1;2;3;4
Ф3	Системи управління інформаційною безпекою	6,0	іс	БІТ	1;2
Ф4	Управління інноваційними проектами	3,0	дз	ПЕППУ	1
1.2.2	<i>Практична підготовка за спеціальністю та атестація</i>	30			
П1	Виробнича практика	8,0	дз	БІТ	5
П2	Передатестаційна практика	4,0	дз	БІТ	5

1	2	3	4	5	6
КР	Виконання кваліфікаційної роботи	17,5		БІТ	
	Виконання кваліфікаційної роботи	0,5		ПЕППУ	
	ВИБІРКОВА ЧАСТИНА	24			
В	Визначається завдяки вибору здобувачами навчальних дисциплін із запропонованого переліку відповідно до ПОЛОЖЕННЯ https://www.nmu.org.ua/ua/content/activity/us_documents/The_choice_of_academic_disciplines_by_students_2020.pdf				
	Разом за обов'язковою та вибірковою частинами	90			

Примітка:

Позначення кафедр, яким доручається викладання дисциплін: БІТ – безпеки інформації та телекомунікацій; ІнМов – іноземних мов; ПЕППУ – прикладної економіки, підприємництва та публічного управління; ОП та ЦБ – охорони праці та цивільної безпеки.

6 СТРУКТУРНО-ЛОГІЧНА СХЕМА

Послідовність навчальної діяльності здобувача за денною формою навчання подана нижче.

Курс	Семестр	Чверть	Шифри освітніх компонентів	Річний обсяг, кредити	Кількість освітніх компонент, що викладаються протягом		
					чверті	семестру	року
1	2	3	4	5	6	7	8
1	1	1	31, 32, Ф1, Ф2, Ф3, Ф4	60	6	6	12
		2	31, Ф1, Ф2, Ф3		4		
	2	3	31, Ф2, В		8	8	
		4	31, Ф2, В		8		
2	3	5	П1, П2, КР	30	3	3	3

Примітка:

Кількість освітніх компонент у чвертях та семестрах з урахуванням вибіркового навчальних дисциплін визначається після обрання навчальних дисциплін здобувачами вищої освіти

8 ПРИКІНЦЕВІ ПОЛОЖЕННЯ

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

1. 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>.

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

3. 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>.

4. 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>.

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

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

7. Закон України «Про освіту» [Електронний ресурс]. <https://zakon.rada.gov.ua/laws/show/2145-19>.

8. 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.

9. Методичні рекомендації щодо розроблення стандартів вищої освіти, затверджених наказом Міністерства освіти і науки України від 01.06.2016 р. № 600 (зі змінами).

10. Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Ліцензійні умови провадження освітньої діяльності закладів освіти». <http://zakon5.rada.gov.ua/laws/show/1187-2015-p/page>.

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

12. Положення про організацію освітнього процесу Національного технічного університету «Дніпровська політехніка» від 25.10.2019 р.

13. Положення про формування переліку та обрання навчальних дисциплін здобувачами вищої освіти Національного технічного університету «Дніпровська політехніка» від 17.01.2020 р.

14. Положення про порядок реалізації права на академічну мобільність

Національного технічного університету “Дніпровська політехніка” від 19.04.2018 р.

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

Освітня програма поширюється на всі кафедри університету та вводиться в дію з 01 вересня 2021 року.

Термін дії освітньої програми не може перевищувати 1 рік 4 місяці та/або період акредитації. Освітня програма підлягає перегляду відповідно до змін нормативної бази України в сфері вищої освіти, але не рідше одного разу на рік.

Відповідальність за якість та унікальні конкурентні переваги освітньої програми несе гарант освітньої програми.

Навчальне видання

Корнієнко Валерій Іванович
Герасіна Олександра Володимирівна
Кагадій Тетяна Станіславівна
Кручинін Олександр Володимирович
Тимофєєв Дмитро Сергійович

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА МАГІСТРА
СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА**

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.