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

ЗАТВЕРДЖЕНО
Вченою радою університету
«» 2022 р., протокол №

Голова Вченої ради
_____ Г.Г. Півняк

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 01.09.2022 р.

Наказ від

Ректор
_____ О.О. Азюковський

Дніпро
НТУ «ДП»
2022

ЛИСТ-ПОГОДЖЕННЯ

Центр моніторингу знань та тестування
протокол № _____ від «__»_____20___ р.

Директор _____ _____.
(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 – керівник робочої групи, гарант програми.
2. Герасіна Олександра Володимирівна, к.т.н., доцентка, доцентка кафедри безпеки інформації та телекомунікацій – членкиня робочої групи.
3. Ковальова Юлія Вікторівна – к.т.н., доцентка кафедри безпеки інформації та телекомунікацій – членкиня робочої групи.
4. Кручінін Олександр Володимирович, старший викладач кафедри безпеки інформації та телекомунікацій – член робочої групи.
5. Тимофєєв Дмитро Сергійович, старший викладач кафедри безпеки інформації та телекомунікацій – член робочої групи.
6. Ангеловський Микола Олександрович, студент групи 125м-21-1.

Рецензії-відгуки зовнішніх стейкхолдерів:

ЗМІСТ

ВСТУП

Освітньо-професійна програма розроблена на основі 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, одиничний, обсяг освітньої програми – 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 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	Інформаційний пакет за спеціальністю https://bit.nmu.org.ua/ua/ Освітні програми НТУ «ДП» http://www.nmu.org.ua/ua/content/infrastructure/structural_divisions/science_met_dep/educational_programs/
1.2 Мета освітньої програми	
Підготовка фахівців з кібербезпеки із забезпеченням органічного поєднання освітньої та інноваційної діяльності, спрямована на здобуття поглиблених теоретичних і практичних знань щодо формування здатності розв'язувати складні наукові та практичні проблеми в галузі інформаційних технологій, 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.	
1.3 Характеристика освітньої програми	
Предметна область	12 Інформаційні технології / 125 Кібербезпека. **Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки.

	Цілі навчання: підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області.** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорії математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології:** методи, моделі, методики та технології 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 професійних задач в галузі інформаційної безпеки та/або кібербезпеки; технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання:** засоби, пристрої, 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 інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна, прикладна та має наступні професійні (спеціалізаційні) акценти: 1. Поглиблене вивчення та застосування законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності. 2. Посилена підготовка в галузі міждисциплінарного системного аналізу із вивченням сучасних методів моделювання складних нелінійних процесів для створення систем захисту інформаційних потоків у комунікаційних мережах. 3. Вивчення та застосування теорії, моделей та принципів управління доступом до інформаційних ресурсів із забезпеченням криптографічного захисту інформації в сучасних інформаційно-комунікаційних технологій. 4. Вивчення та застосування інтелектуальних технологій моделювання процесів в системах кіберзахисту. 5. Формування максимально широкого науково-технічного світогляду майбутнього професіонала.
Основний фокус освітньої програми	Спеціальна освіта в галузі 12 Інформаційні технології / спеціальності 125 Кібербезпека. Підготовка фахівців, здатних до інноваційної науково-

	дослідницької діяльності при дослідженні, проектуванні, модернізації, впровадженні та експлуатації сучасних систем та технологій інформаційної та/або кібербезпеки. Ключові слова: кіберзахист, інформаційна безпека, управління безпекою, інфокомунікаційні системи та мережі
Особливості програми	Виробнича та передатестаційна практика обов'язкові. Проводяться в спеціалізованих комп'ютерних лабораторіях та комп'ютерних класах кафедри, на базі Придніпровського 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 і 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 розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Робота перевіряється на наявність плагіату згідно з процедурою, визначеною системою забезпечення якості освітньої діяльності та якості вищої освіти університету. Захист кваліфікаційної роботи відбувається прилюдно на засіданні екзаменаційної комісії. Кваліфікаційна робота оприлюднюється в репозиторії університету.
1.6 Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Кадрове забезпечення відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності для другого (магістерського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності. До проведення аудиторних занять залучаються професіонали-практики з Придніпровського центру технічного захисту інформації. 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 другого (магістерського) 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	Інформаційне забезпечення передбачає наявність: - вітчизняних та закордонних фахових періодичних видань відповідного профілю у бібліотеці закладу освіти (у тому числі в електронному вигляді) залежно від найвищого рівня, за яким фактично провадиться освітня діяльність; - доступу до баз даних періодичних наукових видань англійською мовою відповідного профілю; - використання професійної дистанційної платформи підготовки фахівців з кібербезпеки; - офіційного вебсайта закладу освіти українською та англійською мовою, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/атестаційна (наукових працівників) діяльність, зразки документів про освіту, умови для доступності осіб з інвалідністю та інших маломобільних груп населення до приміщень, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила

	прийому, контактна інформація). Навчально-методичне забезпечення передбачає наявність: - затверджених освітньо-професійної програми, навчальних планів, за якими здійснюється підготовка здобувачів вищої освіти; робочих програм з усіх навчальних дисциплін навчальних планів; - програм з усіх видів практичної підготовки до кожної освітньої програми; - методичних матеріалів для проведення підсумкової атестації здобувачів вищої освіти тощо. 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**.**
1.7 Академічна мобільність	
Національна кредитна мобільність	Можливість укладання угод про академічну мобільність, про подвійне дипломування тощо
Міжнародна кредитна мобільність	Можливість укладання угод про міжнародну мобільність, про подвійне дипломування, про тривалі міжнародні проекти, що передбачають навчання студентів тощо. Положення про порядок реалізації права на академічну мобільність НТУ "Дніпровська політехніка": **http://surl.li/crwsa** Стратегія інтернаціоналізації НТУ "Дніпровська політехніка": 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 особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

2.1 Загальні компетентності

Шифр	Компетентності
1	***2***
КЗ-1	Здатність застосовувати знання у практичних ситуаціях.
КЗ-2	Здатність проводити дослідження на відповідному рівні.
КЗ-3	Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4	Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

2.2 Спеціальні компетентності

2.2.1 Фахові (спеціальні) компетентності за стандартом вищої освіти

Шифр	Компетентності
1	***2***
КФ1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
КФ4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ8	Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій,

	бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

2.2.2 Спеціальні компетентності з урахуванням особливостей освітньої програми

Шифр	**Компетентності**
1	***2***
СК11	Здатність здійснювати моделювання складних процесів у галузі інформаційної безпеки та/або кібербезпеки із використанням інтелектуальних методів систем штучного інтелекту та проводити дослідження із застосуванням сучасних експериментальних і теоретичних методів.

3 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	**Програмні результати навчання**	**Компетентності**
РН1	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	КЗ1, КЗ3, КФ1
РН2	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	КЗ2, КЗ3, КФ1-КФ3
РН3	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	КЗ1, КФ1
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	КЗ1-КЗ4, КФ1-КФ2
РН5	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	КЗ3, КЗ5, КФ2
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	КЗ1, КЗ4, КФ1, КФ3, КФ5-КФ7, КФ9

РН7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	К31, К33, КФ2
РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	К31, К32, К34, К35, КФ3, КФ9, КФ10
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	К31-К34, КФ4, КФ9, КФ10
РН10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	К31, К33, К34, КФ5, КФ9
РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	К31, К33, К34, КФ6, КФ10
РН12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	К31, К33, К34, КФ4, КФ7, КФ10
РН13	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.	К31, К33, К34, КФ8, КФ10
РН14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	К31, К33, К34, КФ4, КФ9, КФ10
РН15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	К34, К35, КФ10
РН16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	К31-К34, КФ3-КФ7, КФ9, КФ10
РН17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.	КФ3, КФ10
РН18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	К31, К34, К35, КФ10

РН19	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	КЗ1, КЗ4, КЗ5, КФ1-КФ4, КФ6-КФ9
РН20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	КЗ1- КЗ5, КФ1, КФ3
РН21	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	КЗ1-КЗ4, КФ1, КФ3, КФ5, КФ7, КФ8
РН22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	КЗ2-КЗ4, КФ1, КФ3
РН23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	КЗ1, КЗ3, КЗ4, КФ1-КФ3, КФ6-КФ9
	Спеціальні результати навчання з урахуванням особливостей освітньої програми	
РН24	Здійснювати моделювання складних процесів у галузі інформаційної безпеки та/або кібербезпеки із використанням інтелектуальних методів систем штучного інтелекту та проводити дослідження із застосуванням сучасних експериментальних і теоретичних методів.	СК11

4 РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр	**Результати навчання**	**Найменування освітніх компонентів**
1	*2*	*3*
1 ОБОВ'ЯЗКОВА ЧАСТИНА		
РН1	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	Іноземна мова для професійної діяльності (англійська/німецька/французька)
РН2	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних	Виконання кваліфікаційної роботи

1	*2*	*3*
	контекстах.	
РН3	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	Технології забезпечення інформаційної і кібербезпеки об’єктів Виробнича практика
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	Технології забезпечення інформаційної і кібербезпеки об’єктів Інтелектуальні системи кіберзахисту Моделювання складних нелінійних процесів в кібербезпеці
РН5	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	Технології забезпечення інформаційної і кібербезпеки об’єктів Моделювання складних нелінійних процесів в кібербезпеці Передатестаційна практика
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	Технології забезпечення інформаційної і кібербезпеки об’єктів Системи управління інформаційною безпекою Виробнича практика
РН7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	Системи управління інформаційною безпекою Виробнича практика
РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.	Системи управління інформаційною безпекою
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	Системи управління інформаційною безпекою
РН10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	Технології забезпечення інформаційної і кібербезпеки об’єктів
РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно	Виробнича практика

1	*2*	*3*
	до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	
РН12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	Системи управління інформаційною безпекою
РН13	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	Технології забезпечення інформаційної і кібербезпеки об'єктів Моделювання складних нелінійних процесів в кібербезпеці Виробнича практика
РН14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	Системи управління інформаційною безпекою Виробнича практика
РН15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	Іноземна мова для професійної діяльності (англійська/німецька/французька) Управління безпекою, автономність та відповідальність у професійній діяльності Виконання кваліфікаційної роботи
РН16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	Управління безпекою, автономність та відповідальність у професійній діяльності Управління інноваційними проектами Моделювання складних нелінійних процесів в кібербезпеці
РН17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	Управління безпекою, автономність та відповідальність у професійній діяльності Виробнича практика Передатестаційна практика Виконання кваліфікаційної роботи
РН18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	Управління безпекою, автономність та відповідальність у професійній діяльності Управління інноваційними проектами

1	*2*	*3*
РН19	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	Управління інноваційними проектами Інтелектуальні системи кіберзахисту Передатестаційна практика Виконання кваліфікаційної роботи
РН20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	Виконання кваліфікаційної роботи
РН21	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	Моделювання складних нелінійних процесів в кібербезпеці Виконання кваліфікаційної роботи
РН22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	Виконання кваліфікаційної роботи
РН23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	Інтелектуальні системи кіберзахисту Виконання кваліфікаційної роботи
РН24	Здійснювати моделювання складних процесів у галузі інформаційної безпеки та/або кібербезпеки із використанням інтелектуальних методів систем штучного інтелекту та проводити дослідження із застосуванням сучасних експериментальних і теоретичних методів.	Моделювання складних нелінійних процесів в кібербезпеці Інтелектуальні системи кіберзахисту
2 ВИБІРКОВА ЧАСТИНА **Визначається завдяки вибору здобувачами 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*	*5*
1	**ОБОВ'ЯЗКОВА ЧАСТИНА**	**66**		
1.1	**Цикл загальної підготовки**	**9**		
З1	Іноземна мова для професійної діяльності (англійська/ німецька/ французька)	6,0	іс	1;2;3;4
З2	Управління безпекою, автономність та відповідальність у професійній діяльності	3,0	дз	3
1.2	**Цикл спеціальної підготовки**	**57**		
1.2.1	*Фахові освітні компоненти за спеціальністю*	**27**		
Ф1	Технології забезпечення інформаційної і кібербезпеки об'єктів	8,0	іс	1;2
Ф2	Інтелектуальні системи кіберзахисту	5,0	іс	1;2
Ф3	Системи управління інформаційною безпекою	6,0	іс	1;2
Ф4	Управління інноваційними проектами	3,0	дз	1
Ф5	Моделювання складних нелінійних процесів в кібербезпеці	5,0	іс	3;4
1.2.2	*Практична підготовка за спеціальністю та атестація*	**30**		
П1	Виробнича практика	10,0	дз	5
П2	Передатестаційна практика	5,0	дз	5
КР	Виконання кваліфікаційної роботи	14,5		
	Виконання кваліфікаційної роботи	0,5		
	ВИБІРКОВА ЧАСТИНА	**24**		
В	**Визначається завдяки вибору здобувачами навчальних дисциплін із запропонованого переліку**			
	Разом за обов'язковою та вибірковою частинами	**90**		

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	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	1	1	З1, Ф1, Ф2, Ф3, Ф4	60	5	5	13
		2	З1, Ф1, Ф2, Ф3		4		
	2	3	З1, З2, Ф5, В		4	4	
		4	З1, Ф5, В		3		
2	3	5	П1, П2	30	2	2	3
		6	КР		1	1	

Примітка:

Кількість освітніх компонент у чвертях та семестрах з урахуванням вибіркових навчальних дисциплін 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	Ф1	Ф2	Ф3	Ф4	Ф5	П1	П2	КР
Компетентності	КЗ1	+				+			+		
	КЗ2				+			+			+
	КЗ3			+	+	+		+			+
	КЗ4		+	+		+			+	+	+
	КЗ5	+	+				+				+
	КФ1			+	+	+		+			+
	КФ2			+		+			+		+
	КФ3			+		+			+		
	КФ4					+			+		+
	КФ5			+					+		+
	КФ6			+		+					
	КФ7					+			+		
	КФ8			+					+		
	КФ9					+			+		
	КФ10		+				+		+	+	+
	СК11				+			+			

Таблиця 2. Матриця відповідності результатів навчання компонентам освітньої програми

		Компоненти освітньої програми									
		З1	З2	Ф1	Ф2	Ф3	Ф4	Ф5	П1	П2	КР
Результати навчання	РН1	+									
	РН2										+
	РН3			+					+		
	РН4			+	+			+			
	РН5			+				+		+	
	РН6			+		+			+		
	РН7					+			+		
	РН8					+					
	РН9					+					
	РН10			+							
	РН11								+		
	РН12					+					
	РН13			+				+	+		
	РН14					+			+		
	РН15	+	+								+
	РН16		+				+	+			
	РН17		+						+	+	+
	РН18		+				+				
	РН19				+		+			+	+
	РН20										+
	РН21							+			+
	РН22										+
	РН23				+						+
	РН24				+			+			

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 І). [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. Національний класифікатор України: "Класифікатор професій" ДК 003:2010.

9. Національна рамка кваліфікацій – https://zakon.rada.gov.ua/laws/show/1341-2011-п.

10. Перелік галузей знань і спеціальностей – http://zakon4.rada.gov.ua/laws/show/266-2015-п.

11. 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.

12. Методичні рекомендації щодо розроблення стандартів вищої освіти. Затверджено Наказом Міністерства освіти і науки України від 01.06.2017 р. № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584 – https://mon.gov.ua/storage/app/media/vyshcha/naukovo-metodychna_rada/2020metod-rekomendacziyi.docx

13. Постанова Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності». http://zakon5.rada.gov.ua/laws/show/1187-2015-п/page.

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

15. Положення про організацію освітнього процесу Національного технічного університету "Дніпровська політехніка" від 25.10.2019 р.

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

17. Положення про порядок реалізації права на академічну мобільність Національного технічного університету "Дніпровська політехніка" від 19.04.2018 р.

18. Стандарт вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти, затверджений наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

19. Стандарти та рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG) // URL: https://ihed.org.ua/wpcontent/uploads/2018/10/04_2016_ESG_2015.pdf.

20. EQF 2017 (Європейська рамка кваліфікацій) // URL: https://ec.europa.eu/ploteus/sites/eac-eqf/files/en.pdf; https://ec.europa.eu/ploteus/content/descriptors-page.

21. QF EHEA 2018 (Рамка кваліфікацій ЄПВО) // URL: http://www.ehea.info/Upload/document/ministerial_declarations/EHEAParis2018_Communique_AppendixIII_952778.pdf.

22. ISCED (Міжнародна стандартна класифікація освіти, МСКО) 2011 // URL: http://uis.unesco.org/sites/default/files/documents/international-standardclassification-of-education-isced-2011-en.pdf.

23. ISCED-F (Міжнародна стандартна класифікація освіти – Галузі, МСКО-Г) 2013 // URL: http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-fields-of-education-and-training-2013-detailed-field-descriptions-2015-en.pdf.

24. TUNING (для ознайомлення зі спеціальними (фаховими) та загальними компетентностями та прикладами стандартів – http://www.unideusto.org/tuningeu/.

25. Національний освітній глосарій: вища освіта / 2-е вид., перероб. і доп. / авт.-уклад. : В. М. Захарченко, С. А. Калашнікова, В. І. Луговий, А. В. Ставицький, Ю. М. Рашкевич, Ж. В. Таланова / За ред. В. Г. Кременя. – К. : ТОВ "Видавничий дім "Плеяди", 2014.– 100 с. – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskoho-protsesu.html?download=83:hlosarii-terminiv-vyshchoi-osvity-2014-r-onovlene-vydannia-z-urakhuvanniam-polozhen-novoho-zakonu-ukrainy-pro-vyshchu-osvitu&start=80.

26. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-

bolonskoho-protsesu.html?download=82:bolonskyi-protses-nova-paradyhma-vyshchoi-osvity-yu-rashkevych&start=80.

27. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskoho-protsesu.html?download=88:rozvytok-systemy-zabezpechennia-iakosti-vyshchoi-osvity-ukrainy&start=80.

28. Розроблення освітніх програм: методичні рекомендації / Авт.: В.М. Захарченко, В.І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. – К. ДП "НВЦ "Пріоритети", 2014. – 120 с. – http://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskoho-protsesu.html?download=84:rozroblennia-osvitnikh-prohram-metodychni-rekomendatsii&start=80.

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 2022 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
Ковальова Юлія Вікторівна
Кручінін Олександр Володимирович
Тимофєєв Дмитро Сергійович
Ангеловський Микола Олександрович

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.