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

ЗАТВЕРДЖЕНО
Вченою радою університету
«30» червня 2022 р., протокол № 8

Голова Вченої ради
_____ Г.Г. Півняк

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ВИЩОЇ ОСВІТИ
«Кібербезпека»

ГАЛУЗЬ ЗНАНЬ	12 Інформаційні технології
СПЕЦІАЛЬНІСТЬ	125 Кібербезпека
РІВЕНЬ ВИЩОЇ ОСВІТИ	Перший (бакалаврський)
СТУПІНЬ	Бакалавр
ОСВІТНЯ КВАЛІФІКАЦІЯ	Бакалавр з кібербезпеки

Уводиться в дію з 01.09.2022 р.

Наказ від 30 червня 2022 р. № 8-ВР

Ректор
_____ О.О. Азюковський

Дніпро
НТУ «ДП»
2022

ЛИСТ-ПОГОДЖЕННЯ

Центр моніторингу знань та тестування
протокол № 4 від «20» 03 2022 р.
Директор _____ (підпис) Ярової М.М. (ініціали, прізвище)

Відділ внутрішнього забезпечення якості вищої освіти
протокол № 4 від «20» 03 2022 р.
Начальник відділу _____ (підпис) О.О. Яворська (ініціали, прізвище)

Навчально-методичний відділ
протокол № 4 від «20» 03 2022 р.
Начальник відділу _____ (підпис) Заболотна Ю.О. (ініціали, прізвище)

Науково-методична комісія спеціальності 125 Кібербезпека
Протокол № 4 від «22» 02 2022 р.
Голова науково-методичної комісії спеціальності _____ (підпис) В.І. Корнієнко (ініціали, прізвище)

Гарант освітньої програми _____ (підпис) О.В. Герасіна (ініціали, прізвище)

Кафедра безпеки інформації та телекомунікацій
Протокол № 7 від «22» 02 2022 р.
Завідувач кафедри _____ (підпис) В.І. Корнієнко (ініціали, прізвище)

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

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Герасіна Олександра Володимирівна, к.т.н., доцент, доцент кафедри безпеки інформації та телекомунікацій – керівник робочої групи, гарант програми.
2. Корнієнко Валерій Іванович, д.т.н., професор, завідувач кафедри безпеки інформації та телекомунікацій – член робочої групи.
3. Кагадій Тетяна Станіславівна, д.ф.-м.н., професор, професор кафедри безпеки інформації та телекомунікацій – член 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. Самойлік Денис Вікторович, студент групи 125-19-1.

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Бут Сергій Миколайович, помічник генерального директора ДП «КБ «Південне» з безпеки.
2. Єсін Валерій Миколайович, директор ТОВ «Спеціальні захисні системи».

ЗМІСТ

ВСТУП

Освітньо-професійна програма розроблена на основі Стандарту вищої освіти підготовки бакалаврів 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 бакалаврів 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 бакалаврів спеціальності 125 Кібербезпека;

– екзаменаційна комісія спеціальності 125 Кібербезпека;

– приймальна комісія НТУ «ДП».

Освітня програма поширюється на кафедри університету, які беруть участь у підготовці фахівців ступеня бакалавра спеціальності 125 Кібербезпека.

1 ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

1.1 Загальна інформація	
Повна назва закладу вищої освіти та інституту (факультету)	Національний технічний університет «Дніпровська політехніка», факультет інформаційних технологій, кафедра безпеки інформації та телекомунікацій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньо-професійної програми 240 кредитів ЄКТС. На базі освітньо-кваліфікаційного рівня «молодший спеціаліст» визнаються та перезараховуються 60 кредитів ЄКТС, отриманих у межах попередньої освітньої програми підготовки молодшого спеціаліста Термін навчання – на основі повної загальної середньої освіти – 3 роки 10 місяців; на основі освітньо-кваліфікаційного рівня «молодший спеціаліст» – 2 роки 10 місяців
Наявність акредитації	Міністерство освіти і науки України, Україна. Сертифікат про акредитацію спеціальності УД 04002554 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 2027 р. Акредитація освітньої програми не проводилася
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Особа має право здобувати ступінь бакалавра за умови наявності в неї повної загальної середньої освіти /освітньо-кваліфікаційного рівня «молодший спеціаліст». 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 3 роки 10 місяців 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 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 розробки, використання і впровадження 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 наукові та практичні проблеми в області кібербезпеки із еволюцією освітньо-наукового простору 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 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, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, формування у випускників здатності вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки. 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; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна, прикладна та має наступні професійні (спеціалізаційні) акценти: 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. Підготовка зі створення комплексних систем захисту інформаційних потоків у комунікаційних мережах; 4. Розвиток знань у галузі кібернетичної безпеки на основі аналізу нових науково-технологічних здобутків; 5. Ознайомлення з новими напрямками кібернетичної безпеки для навчання здобувачів вищої освіти розробці індивідуальних стартапів на етапі підготовки кваліфікаційної роботи.
Основний фокус освітньої програми	Спеціальна освіта в галузі 12 Інформаційні технології / спеціальності 125 Кібербезпека. Підготовка фахівців, здатних розробляти, використовувати і впроваджувати технології інформаційної та/або кібербезпеки в інформаційно-комунікаційних системах та мережах. Ключові слова: інформаційні технології, управління інформаційною і кібербезпекою, технічний захист інформації
Особливості програми	Навчальна, виробнича та передатестаційна практики

	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 розробку, використання і впровадження систем та технологій інформаційної та кібербезпеки інфокомунікаційних систем і мереж та критичної інформаційної інфраструктури.
1.4 Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Види економічної діяльності за класифікатором ДК 009:2010: Секція J Інформація та телекомунікації, 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 – 7, рівень FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
1.5 Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання. 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 здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи бакалавра.

	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом за спеціальністю 125 Кібербезпека та цією освітньою програмою. Кваліфікаційний проект/робота передбачає розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки. 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 репозитарії університету.
1.6 Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Кадрове забезпечення відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності для першого (бакалаврського) рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності. До проведення аудиторних занять залучаються професіонали-практики з Придніпровського регіонального науково-технічного 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 першого (бакалаврського) 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	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність. 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання. Специфічними характеристиками інформаційного та навчально-методичного забезпечення є використання національних та міжнародних стандартів в галузі інформаційної та кібербезпеки. 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. За необхідності заняття та атестація здобувачів вищої освіти проводяться з використанням платформ Zoom та MS Teams.
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 Міжнародну кредитну мобільність регламентують відповідні документи: Положення про порядок реалізації права на академічну мобільність НТУ "Дніпровська політехніка": http://surl.li/ajzjq 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 бакалавра зі спеціальності 125 Кібербезпека - Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

2.1 Загальні компетентності за стандартом вищої освіти

Шифр	**Компетентності**
1	***2***
К31	Здатність застосовувати знання у практичних ситуаціях
К32	Знання та розуміння предметної області та розуміння професії.
К33	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і

1	*2*
	письмово.
КЗ4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КЗ5	Здатність до пошуку, оброблення та аналізу інформації.
КЗ6	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КЗ7	Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

2.2 Спеціальні (фахові) компетентності за стандартом вищої освіти

Шифр	**Компетентності**
1	*2*
КФ1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
КФ2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
КФ5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
КФ7	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
КФ8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
КФ11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

3 НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ

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

Шифр	**Результати навчання**
1	***2***
РН1	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
РН2	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
РН3	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН4	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН5	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
РН6	Реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. - критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
РН7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН8	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки. - виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
РН9	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; - розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; - застосовувати в професійній діяльності знання, навички та практики, щодо

1	*2*
	структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; - здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційно телекомунікаційних системах. - впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
РН10	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
РН11	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; - розробляти моделі загроз та порушника.
РН12	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-

1	*2*
	телекомунікаційних (автоматизованих) системах.
РН13	- вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; - вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес процесів після здійснення кібератак, збоїв та відмов різних класів. - створювати і впроваджувати плани процесу забезпечення безперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання;
РН14	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання та ін.) наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі експертизи, випробування комплексних систем захисту інформації
РН15	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;
РН16	- забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; - забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;
РН17	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; - обґрунтовувати можливість створення технічних каналів витоку інформації на об’єктах інформаційної діяльності;

1	*2*
	- впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;
РН18	- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем; - забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах;
РН19	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

4 РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр РН	**Результати навчання**	**Найменування освітніх компонентів**
1	*2*	*3*
1 ОБОВ'ЯЗКОВА ЧАСТИНА		
РН1	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;	Ціннісні компетенції фахівця Вступ до фаху Практика навчальна комп'ютерна Практика технологічна Виробнича практика
РН2	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;	Ціннісні компетенції фахівця Вступ до фаху
РН3	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації	Українська мова Іноземна мова професійного спрямування (англійська / німецька / французька) Іноземна мова (для професійних цілей)
РН4	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;	Ціннісні компетенції фахівця Правознавство Цивільна безпека
РН5	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;	Ціннісні компетенції фахівця Вступ до фаху
РН6	Реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та	Цивілізаційні процеси в українському суспільстві Ціннісні компетенції фахівця

1	*2*	*3*
	необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	Фізична культура та спорт
РН7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.	Цивілізаційні процеси в українському суспільстві Правознавство
РН8	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.	Кіберзахист Комплексні системи захисту інформації
РН9	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; - розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; - застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; - здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційнотелекомунікаційних системах.	Вища математика Теорія ймовірностей та математична статистика Спеціальні розділи з математики Кіберзахист Інформаційні технології Мережеві технології і протоколи Архітектура комп’ютерів Операційні системи Практика навчальна комп'ютерна Практика технологічна
РН10	- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.	Фізика Програмування і алгоритмічні мови Кіберзахист Прикладна криптологія Цифрова стеганографія
РН11	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління	Кіберзахист Мережеві технології і

1	*2*	*3*
	доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.	протоколи Управління інформаційною безпекою Цифрова стеганографія
РН12	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.	Економіка і управління підприємством Комплексні системи захисту інформації Виробнича практика
РН13	- вирішувати задачі управління процесами	Економіка і управління

1	*2*	*3*
	забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; - вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес процесів після здійснення кібератак, збоїв та відмов різних класів. - створювати і впроваджувати плани процесу забезпечення безперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання;	підприємством Управління інформаційною безпекою
РН14	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання та ін.) наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі експертизи, випробування комплексних систем захисту інформації	Комплексні системи захисту інформації
РН15	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;	Кіберзахист Управління інформаційною безпекою
РН16	- забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; - забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;	Управління інформаційною безпекою Економіка і управління підприємством
РН17	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації;	Виробнича практика Передатестаційна практика Виконання кваліфікаційної

1	*2*	*3*
	- аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; - обґрунтовувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; - впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;	роботи Спеціальні розділи з математики Основи електроніки Прикладна криптологія
РН18	- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем; - забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах;	Управління інформаційною безпекою
РН19	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.	Виробнича практика Передатестаційна практика Виконання кваліфікаційної роботи Управління інформаційною безпекою
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**	**180**		
1.1	**Цикл загальної підготовки**	**30**		
З1	Українська мова	3,0	іс	1
З2	Цивілізаційні процеси в українському суспільстві	3,0	дз	3
З3	Іноземна мова професійного спрямування (англійська / німецька / французька)	6,0	іс	1;2;3;4
З4	Ціннісні компетенції фахівця	6,0	іс	7;8
З5	Фізична культура і спорт	6,0	дз	1;2;3;4 5;6;7;8
З6	Правознавство	3,0	дз	9
З7	Цивільна безпека	3,0	іс	14
1.2	**Цикл спеціальної підготовки**	**150**		
1.2.1	*Базові дисципліни за галуззю знань*	**23**		
Б1	Вища математика	8,0	іс	1;2;3;4
Б2	Фізика	8,0	іс	1;2;3;4
Б3	Теорія ймовірностей та математична статистика	4,0	дз	7;8
Б4	Економіка і управління підприємством	3,0	дз	15
1.2.2	*Фахові освітні компоненти за спеціальністю*	**97**		
Ф1	Спеціальні розділи з математики	4,0	дз	5;6
	Спеціальні розділи з математики	6,0	іс	7;8
Ф2	Вступ до фаху	3,0	дз	1
Ф3	Програмування і алгоритмічні мови	11,0	іс	1;2;3;4
Ф4	Основи електроніки	5,0	дз	5;6
Ф5	Кіберзахист	10,0	іс	13;14; 15
Ф6	Інформаційні технології	5,0	дз	1;2
Ф7	Мережеві технології і протоколи	8,0	іс	7,8
Ф8	Комплексні системи захисту інформації	10,0	іс	15
Ф9	Архітектура комп'ютерів	4,0	дз	3;4
Ф10	Операційні системи	6,0	іс	5;6
Ф11	Іноземна мова (для професійних цілей)	6,0	дз	9;10; 11;12
Ф12	Прикладна криптологія	9,0	іс	9;10; 11;12
Ф13	Управління інформаційною безпекою	5,0	іс	13;14
Ф14	Цифрова стеганографія	5,0	іс	15
1.2.3	*Практична підготовка за спеціальністю та атестація*	**30**		
П1	Практика навчальна комп'ютерна	6,0	дз	4
П2	Практика технологічна	6,0	дз	8
П3	Виробнича практика	6,0	дз	12
П4	Передатестаційна практика	3,0	дз	16

1	*2*	*3*	*4*	*5*
КР	Виконання кваліфікаційної роботи	8,5		16
	Виконання кваліфікаційної роботи	0,5		16
	ВИБІРКОВА ЧАСТИНА	**60**		
В	**Визначається завдяки вибору здобувачами навчальних дисциплін із запропонованого переліку**			
	Разом за обов'язковою та вибірковою частинами	**240**		

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	З1, З3, З5, Б1, Б2, Ф2, Ф3, Ф6	60	8	8	11
		2	З3, З5, Б1, Б2, Ф3, Ф6		6		
	2	3	З2, З3, З5, Б1, Б2, Ф3, Ф9		7	8	
		4	З3, З5, Б1, Б2, Ф3, Ф9, П1		7		
2	3	5	З5, Ф1, Ф4, Ф10, В	60	5	5	12
		6	З5, Ф1, Ф4, Ф10, В		5		
	4	7	З4, З5, Б3, Ф1, Ф7, В		6	7	
		8	З4, З5, Б3, Ф1, Ф7, П2, В		7		
3	5	9	З6, Ф11, Ф12, В	60	4	4	13
		10	Ф11, Ф12, В		3		
	6	11	Ф11, Ф12, В		3	4	
		12	Ф11, Ф12, П3, В		4		
4	7	13	Ф5, Ф13, В	60	3	4	12
		14	З7, Ф5, Ф13, В		4		
	8	15	Б4, Ф5, Ф8, Ф14		4	6	
		16	П4, КР		2		

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	З3	З4	З5	З6	З7	Б1	Б2	Б3	Б4	Ф1	Ф2	Ф3	Ф4	Ф5	Ф6	Ф7	Ф8	Ф9	Ф10	Ф11	Ф12	Ф13	Ф14	П1	П2	П3	П4	КР
Компетентності	КЗ1				*									*													*	*	*	*	
	КЗ2				*									*																	
	КЗ3	*		*																			*								
	КЗ4				*		*	*																							
	КЗ5				*									*																	*
	КЗ6		*		*		*																								
	КЗ7		*			*	*	*																							
	КФ1						*										*			*											
	КФ2								*		*		*				*	*	*		*	*					*	*			
	КФ3									*					*		*							*		*					
	КФ4											*					*		*						*	*					
	КФ5											*								*									*		
	КФ6																*								*						
	КФ7																			*											
	КФ8																*								*						
	КФ9																								*						
	КФ10												*			*							*						*	*	*
	КФ11																								*						
	КФ12																								*				*	*	*

Таблиця 2. Матриця відповідності результатів навчання компонентам освітньої програми

		Компоненти освітньої програми																														
		З1	З2	З3	З4	З5	З6	З7	Б1	Б2	Б3	Б4	Ф1	Ф2	Ф3	Ф4	Ф5	Ф6	Ф7	Ф8	Ф9	Ф10	Ф11	Ф12	Ф13	Ф14	П1	П2	П3	П4	КР
Результати навчання	РН1				*									*													*	*	*		
	РН2				*									*																	
	РН3	*		*																			*								
	РН4				*		*	*																							
	РН5				*									*																	
	РН6		*		*	*																									
	РН7		*				*																								
	РН8																*			*											
	РН9								*		*		*				*	*	*		*	*					*	*			
	РН10									*					*		*							*		*					
	РН11																*		*						*	*					
	РН12											*								*									*		
	РН13											*													*						
	РН14																			*											
	РН15																*								*						
	РН16											*													*						
	РН17												*			*								*					*	*	*
	РН18																								*						
	РН19																								*				*	*	*

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. 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. Стандарт вищої освіти підготовки бакалавра зі спеціальності 125 «Кібербезпека». СВО-2018. – К. : МОН України, 2018. – 19 с. – Введено в дію наказом МОН України від 04.10.2018р. № 1074.

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

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" від 25.10.2019 р.

14. Положення про формування переліку та обрання навчальних дисциплін

здобувачами вищої освіти Національного технічного університету “Дніпровська політехніка” від 17.01.2020 р.

15. 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 2022 року.

Термін дії освітньої програми не може перевищувати 3 роки 10 місяців 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

Герасіна Олександра Володимирівна
Корнієнко Валерій Іванович
Кагадій Тетяна Станіславівна
Кручінін Олександр Володимирович
Тимофєєв Дмитро Сергійович
Самойлік Денис Вікторович

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА « БАКАЛАВРА 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.

Рецензія стейкхолдера
на освітньо-професійну програму «Кібербезпека»
підготовки бакалаврів зі спеціальності 125 «Кібербезпека» в
Національному технічному університеті «Дніпровська політехніка»

Основним завданням сучасних закладів вищої освіти є надання якісної освіти через впровадження компетентнісного підходу, оскільки його реалізація передбачає формування здатності до використання здобутих освітніх знань, вмінь у професійній практичній підготовці. Освітня програма передбачає формування загальних та спеціальних компетентностей, що вирішується через навчання та практичну підготовку, які відбуваються у активному освітньому середовищі.

Проведений аналіз показує, що освітньо-професійна програма (ОПП) чітко структурована і містить: опис профілю програми; перелік компонентів ОПП та їх логічну послідовність; форми атестації здобувачів вищої освіти; матрицю відповідності програмних компетентностей компонентам ОПП; таблицю забезпечення програмних результатів навчання відповідними освітніми компонентами.

Програма має на меті підготовку фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Її реалізація здійснюється через формування у випускників здатності вирішувати спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.

Заслуговує на увагу чітке визначення результатів освітньої діяльності. До основних компетентностей здобувачів вищої освіти віднесено інтегральну компетентність, як здатність розв'язувати спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. Аналіз ресурсного забезпечення свідчить про достатню практичну спрямованість професійної підготовки, а також створення сучасного освітнього середовища, що відповідає чинним нормам і забезпечує проведення всіх видів навчальної та науково-дослідницької роботи студентів.

Освітньо-професійна програма відповідає стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти та містить обов'язкові та вибіркові компоненти, передбачає достатню кількість часу на теоретичну і практичну підготовку студентів.

Усе вищевикладене дає підстави для висновку, що представлена освітньо-професійна програма містить усі необхідні компоненти, відповідає стандарту вищої освіти та вимогам до розроблення освітніх програм і, таким чином, рекомендується для впровадження в освітній процес НТУ «Дніпровська політехніка».

Стейкхолдер:

Помічник Генерального директора
ДП «КБ «Південне» з безпеки С.М. Бут

Рецензія стейкхолдера
на освітньо-професійну програму «Кібербезпека»
підготовки бакалаврів зі спеціальності 125 «Кібербезпека» в
Національному технічному університеті «Дніпровська політехніка»

Основним завданням сучасних закладів вищої освіти є надання якісної освіти через впровадження компетентнісного підходу, оскільки його реалізація передбачає формування здатності до використання здобутих освітніх знань, вмінь у професійній практичній підготовці. Освітня програма передбачає формування загальних та спеціальних компетентностей, що вирішується через навчання та практичну підготовку, які відбуваються у активному освітньому середовищі.

Проведений аналіз показує, що освітньо-професійна програма (ОПП) чітко структурована і містить: опис профілю програми; перелік компонентів ОПП та їх логічну послідовність; форми атестації здобувачів вищої освіти; матрицю відповідності програмних компетентностей компонентам ОПП; таблицю забезпечення програмних результатів навчання відповідними освітніми компонентами.

Програма має на меті підготовку фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Її реалізація здійснюється через формування у випускників здатності вирішувати спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.

Заслуговує на увагу чітке визначення результатів освітньої діяльності. До основних компетентностей здобувачів вищої освіти віднесено інтегральну компетентність, як здатність розв'язувати спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. Аналіз ресурсного забезпечення свідчить про достатню практичну спрямованість професійної підготовки, а також створення сучасного освітнього середовища, що відповідає чинним нормам і забезпечує проведення всіх видів навчальної та науково-дослідницької роботи студентів.

Освітньо-професійна програма відповідає стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти та містить обов'язкові та вибіркові компоненти, передбачає достатню кількість часу на теоретичну і практичну підготовку студентів.

Усе вищевикладене дає підстави для висновку, що представлена освітньо-професійна програма містить усі необхідні компоненти, відповідає стандарту вищої освіти та вимогам до розроблення освітніх програм і, таким чином, рекомендується для впровадження в освітній процес НТУ «Дніпровська політехніка».

Стейкхолдер:
Директор ТОВ
«Спеціальні захисні системи» В.М.Єсін