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

ЗАТВЕРДЖЕНО
Вченою радою університету
«01» липня 2025 року, протокол № 9
(зі змінами, що затверджені Вченою Радою 21.08.2026 р, протокол № 20)
Голова Вченої ради
_____ Геннадій ПІВНЯК
«21» 08 2026 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ВИЩОЇ ОСВІТИ
«Кібербезпека»

ГАЛУЗЬ ЗНАНЬ	F Інформаційні технології
СПЕЦІАЛЬНІСТЬ	F5 Кібербезпека та захист інформації
РІВЕНЬ ВИЩОЇ ОСВІТИ	Перший (бакалаврський)
СТУПІНЬ	Бакалавр
ОСВІТНЯ КВАЛІФІКАЦІЯ	Бакалавр з кібербезпеки та захисту інформації

Уводиться в дію з 01.09.2025 р.

Наказ від «01» липня 2025 р. № 104
(зі змінами, Наказ від 21.08.2026 № 133)

Ректор
_____ Олександр АЗЮКОВСЬКИЙ

Дніпро
НТУ «ДП»
2025

ЛИСТ-ПОГОДЖЕННЯ

Центр моніторингу знань та тестування
протокол № 8 від «16» 07 2026 р.
Директор _____ Одновол М.М.
(підпис) (ініціали, прізвище)

Відділ внутрішнього забезпечення якості вищої освіти
протокол № 8 від «16» 07 2026 р.
Начальник відділу _____ Т.В. Момотова.
(підпис) (ініціали, прізвище)

Навчально-методичний відділ
протокол № 8 від «16» 07 2026 р.
Начальник відділу _____ Ю.О. Заболотна.
(підпис) (ініціали, прізвище)

Науково-методична комісія спеціальності F5 Кібербезпека та захист інформації
Протокол № 5 від «04» 07 2026 р.
Голова науково-методичної комісії спеціальності _____ В.І. Корнієнко
(підпис) (ініціали, прізвище)

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

Кафедра безпеки інформації та телекомунікацій
Протокол № 13 від «06» 07 2026 р.
Завідувач кафедри _____ В.І. Корнієнко
(підпис) (ініціали, прізвище)

В.о. декана факультету
інформаційних технологій _____ І.Г. Олішевський
(підпис) (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. Іванькова Марія Сергіївна, студентка групи 125-21-5.

Рецензії-відгуки зовнішніх стейкхолдерів:

1. Юрій Пономаренко, начальник сектору захисту критичної інфраструктури Управління Держспецзв’язку у Дніпропетровській області, підполковник.
2. Єсін Валерій Миколайович, директор ТОВ «Спеціальні захисні системи».

ЗМІСТ

ВСТУП 5

1 ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ 5

2 ОБОВ’ЯЗКОВІ КОМПЕТЕНТНОСТІ 11

3 НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ 12

4 РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ 14

5 РОЗПОДІЛ ОБСЯГУ ПРОГРАМИ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ 17

6 СТРУКТУРНО-ЛОГІЧНА СХЕМА 18

7 МАТРИЦІ ВІДПОВІДНОСТІ 19

8 ПРИКІНЦЕВІ ПОЛОЖЕННЯ 21

ДОДАТКИ 24

ВСТУП

Освітньо-професійна програма розроблена на основі Стандарту вищої освіти підготовки бакалаврів спеціальності 125 Кібербезпека (наказ Міністерства освіти і науки України від 04.10.2018 № 1074) з урахуванням зміни назви спеціальності 125 Кібербезпека та захист інформації (Постанова Кабінету Міністрів України від 16 грудня 2022 р. № 1392), наказу МОН України від 13.06.2024 №842 «Про внесення змін до деяких стандартів вищої освіти», наказу МОН України від 29.10.2024 № 1547 «Про внесення змін до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти».

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 F5 Кібербезпека та захист інформації;

– 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 F5 Кібербезпека та захист інформації;

– екзаменаційна комісія спеціальності F5 Кібербезпека та захист інформації;

– приймальна комісія НТУ «ДП».

Освітня програма поширюється на кафедри університету, які беруть участь у підготовці фахівців ступеня бакалавра спеціальності F5 Кібербезпека та захист інформації.

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	Бакалавр Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Кібербезпека

Форма здобуття вищої освіти	Очна (денна), заочна
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний. Обсяг освітньо-професійної програми 240 кредитів ЄКТС. На базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») визнаються та перезараховуються 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). На основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти. Термін навчання – на основі повної загальної середньої освіти – 3 роки 10 місяців; на основі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»), «фаховий молодший бакалавр» – 2 роки 10 місяців
Наявність акредитації	Міністерство освіти і науки України. Сертифікат про акредитацію спеціальності УД № 04020510 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), (на підставі наказу МОН України від 19.11.2024 №1625) 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 / ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») / ступеня «фаховий молодший бакалавр» 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 та практичної діяльності з інтеграцією до міжнародного науково-освітнього простору, яка направлена на	

здобуття поглиблених теоретичних і практичних знань щодо формування здатності розв'язувати фахові задачі в області інформаційної та/або кібербезпеки.	
1.3 Характеристика освітньої програми	
Предметна область	F Інформаційні технології / F5 Кібербезпека та захист інформації Об'єкти вивчення: – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області. Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології: методи, методики та технології розв'язування теоретичних і практичних задач кібербезпеки та захисту інформації. Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
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 F Інформаційні технології / спеціальності F5 Кібербезпека та захист інформації. Підготовка фахівців, здатних розробляти, використовувати і впроваджувати технології інформаційної та/або кібербезпеки в

	інформаційно-комунікаційних системах та мережах, зокрема, об'єктів критичної інфраструктури. 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	На посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації 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. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
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 захист інформації та цією освітньою програмою. Кваліфікаційна робота передбачає розв'язання спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. 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	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді.

навчально-методичного забезпечення	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	Передбачено навчання іноземних здобувачів вищої освіти українською мовою

2 ОБОВ ′ЯЗКОВІ КОМПЕТЕНТНОСТІ

Інтегральна компетентність бакалавра зі спеціальності F5 Кібербезпека та захист інформації - здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

2.1 Загальні компетентності за стандартом вищої освіти

Шифр	**Компетентності**
1	***2***
ЗК1	Здатність застосовувати знання у практичних ситуаціях
ЗК2	Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК3	Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4	Здатність спілкуватися іноземною мовою.
ЗК5	Здатність вчитися і оволодівати сучасними знаннями.
ЗК6	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.
ЗК7	Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
ЗК8	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.
ЗК9	Здатність до національного спротиву

2.2 Спеціальні (фахові, предметні) компетентності за стандартом вищої освіти

Шифр	**Компетентності**
1	***2***
СК1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності.
СК2	Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
СК3	Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
СК4	Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних згідно встановленої політики кібербезпеки й захисту інформації.
СК5	Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
СК6	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо)
СК7	Здатність здійснювати професійну діяльність на основі впровадженої системи

1	*2*
	управління інформаційною та кібербезпекою.
СК8	Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.
СК9	Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.
СК10	Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

3 НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Кінцеві, підсумкові та інтегративні результати навчання бакалавра зі спеціальності F5 Кібербезпека та захист інформації, що визначають нормативний зміст підготовки і корелюються з переліком загальних і спеціальних компетентностей, подано нижче.

Шифр	**Результати навчання**
1	*2*
РН1	Вільно спілкуватися державною мовою усно і письмова при виконанні професійних обов’язків.
РН2	Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
РН3	Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
РН4	Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних завдань у професійній діяльності, оцінювати їхню ефективність.
РН5	Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6	Адаптуватися но нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7	Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8	Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН9	Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10	Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та системи захисту інформації для здійснення професійної діяльності.

1	*2*
РН11	Планувати підготовку та забезпечувати безперервність бізнес процесів в організаціях згідно зі встановленої політикою кібербезпеки з урахуванням вимог до захисту інформації.
РН12	Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно да встановленої політики інформаційної безпеки.
РН13	Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.
РН14	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і відновлення інформації.
РН15	Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН16	Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН17	Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур їх кількісної і якісної оцінки ризиків.
РН18	Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.
РН19	Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН20	Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
РН21	Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
РН22	Набути знання із засадничих та правових аспектів національного спротиву, опанувати комплекс теоретичних знань і практичних навичок, необхідних для виконання конституційного обов’язку із захисту Вітчизни, незалежності та територіальної цілісності України.

4 РОЗПОДІЛ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА ОСВІТНІМИ КОМПОНЕНТАМИ

Шифр РН	**Результати навчання**	**Найменування освітніх компонентів**
1	***2***	***3***
1 ОБОВ'ЯЗКОВА ЧАСТИНА		
РН1	Вільно спілкуватися державною мовою усно і письмова при виконанні професійних обов'язків.	Українська мова
РН2	Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	Іноземна мова професійного спрямування (англійська / німецька / французька)
РН3	Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.	Правознавство
РН4	Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних завдань у професійній діяльності, оцінювати їхню ефективність.	Ціннісні компетенції фахівця Правознавство Цивільна безпека Фізична культура і спорт
РН5	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань 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
РН6	Адаптуватися но нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.	Ціннісні компетенції фахівця Вступ до фаху
РН7	Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.	Теорія ймовірностей та математична статистика Криптологія Цифрова стеганографія Основи кібербезпеки та захисту інформації Основи електроніки Практика технологічна
РН8	Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.	Вища математика Фізика Спеціальні розділи з математики
РН9	Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації	Цивілізаційні процеси в українському суспільстві Правознавство
РН10	Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та системи захисту інформації для здійснення професійної діяльності.	Інформаційні технології Практика навчальна комп'ютерна
РН11	Планувати підготовку та забезпечувати	Управління інформаційною

1	*2*	*3*
	безперервність бізнес процесів в організаціях згідно зі встановленої політикою кібербезпеки з урахуванням вимог до захисту інформації.	безпекою Економіка і управління підприємством
РН12	Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно да встановленої політики інформаційної безпеки.	Кіберзахист Мережеві технології і протоколи Виробнича практика Передатестаційна практика Виконання кваліфікаційної роботи
РН13	Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.	Програмування і алгоритмічні мови Практика навчальна комп'ютерна Операційні системи Мережеві технології і протоколи
РН14	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту і відновлення інформації.	Кіберзахист Мережеві технології і протоколи Управління інформаційною безпекою Програмування і алгоритмічні мови Криптологія Цифрова стеганографія
РН15	Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.	Кіберзахист Виробнича практика Передатестаційна практика Виконання кваліфікаційної роботи
РН16	Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	Комплексні системи захисту інформації
РН17	Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур їх кількісної і якісної оцінки ризиків.	Управління інформаційною безпекою Основи кібербезпеки та захисту інформації
РН18	Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.	Криптологія Цифрова стеганографія Передатестаційна практика Виконання кваліфікаційної роботи
РН19	Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	Криптологія Виконання кваліфікаційної роботи
РН20	Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної	Архітектура комп’ютерів Системи технічного захисту

1	*2*	*3*
	діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.	інформації Комплексні системи захисту інформації Передатестаційна практика Виконання кваліфікаційної роботи
РН21	Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	Виробнича практика Передатестаційна практика Виконання кваліфікаційної роботи Управління інформаційною безпекою Кіберзахист Комплексні системи захисту інформації
РН22	Набути знання із засадничих та правових аспектів національного спротиву, опанувати комплекс теоретичних знань і практичних навичок, необхідних для виконання конституційного обов'язку із захисту Вітчизни, незалежності та територіальної цілісності України	Основи національного спротиву
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	3,0	дз	1;2;3;4
З6	Правознавство	3,0	дз	9
З7	Цивільна безпека	3,0	іс	14
З8	Основи національного спротиву	3,0	дз	7
1.2	**Цикл спеціальної підготовки**	**150**		
1.2.1	*Базові дисципліни*	**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	6,0	іс	5;6
Ф2	Вступ до фаху	3,0	дз	2
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	3;4
Ф7	Мережеві технології і протоколи	8,0	іс	7,8
Ф8	Комплексні системи захисту інформації	9,0	іс	15
Ф9	Архітектура комп'ютерів	4,0	дз	1;2
Ф10	Операційні системи	6,0	іс	5;6
Ф11	Системи технічного захисту інформації	6,0	дз	11;12
Ф12	Криптологія	9,0	іс	9;10; 11;12
Ф13	Управління інформаційною безпекою	5,0	іс	13;14
Ф14	Цифрова стеганографія	6,0	іс	15
Ф15	Основи кібербезпеки та захисту інформації	4,0	дз	5;6
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

1	*2*	*3*	*4*	*5*
П4	Передатестаційна практика	3,0	дз	16
КР	Виконання кваліфікаційної роботи	9,0		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 обов'язковою частиною ОП 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, Ф3, Ф9	60	7	8	11
		2	З3, З5, Б1, Б2, Ф2, Ф3, Ф9		7		
	2	3	З2, З3, З5, Б1, Б2, Ф3, Ф6		7	8	
		4	З3, З5, Б1, Б2, Ф3, Ф6, П1		7		
2	3	5	Ф1, Ф4, Ф10, Ф15, (В)	60	4	4	9
		6	Ф1, Ф4, Ф10, Ф15, (В)		4		
	4	7	З4, З8, Б3, Ф7, (В)		4	5	
		8	З4, Б3, Ф7, П2, (В)		4		
3	5	9	З6, Ф12, (В)	60	2	2	4
		10	Ф12, (В)		1		
	6	11	Ф11, Ф12, (В)		2	3	
		12	Ф11, Ф12, П3, (В)		3		
4	7	13	Ф5, Ф13, (В)	60	2	3	8
		14	З7, Ф5, Ф13, (В)		3		
	8	15	Б4, Ф5, Ф8, Ф14, (В)		4	6	
		16	П4, КР		2		

Примітка:

Кількість освітніх компонент у чвертях та семестрах з урахуванням вибіркових навчальних дисциплін (В) визначається після обрання навчальних дисциплін здобувачами вищої освіти

7 МАТРИЦІ ВІДПОВІДНОСТІ

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

		Компоненти освітньої програми																															
		З1	З2	З3	З4	З5	З6	З7	З8	Б1	Б2	Б3	Б4	Ф1	Ф2	Ф3	Ф4	Ф5	Ф6	Ф7	Ф8	Ф9	Ф10	Ф11	Ф12	Ф13	Ф14	Ф15	П1	П2	П3	П4	КР
Компетентності	ЗК1				*										*														*	*	*	*	
	ЗК2				*										*																			
	ЗК3	*																																
	ЗК4			*																														
	ЗК5				*										*																			*
	ЗК6		*		*		*		*																									
	ЗК7						*																											
	ЗК8		*			*	*	*	*																									
	ЗК9								*																									
	СК1						*											*			*													
	СК2									*		*		*				*	*	*		*	*					*	*	*				
	СК3												*					*		*						*	*							
	СК4												*								*					*					*			
	СК5																	*								*								
	СК6																				*					*								
	СК7																									*								
	СК8													*											*						*	*	*	
	СК9																*							*						*	*	*	
	СК10																									*					*	*	*	

Таблиця 2. Матриця відповідності результатів навчання компонентам освітньої програми

		Компоненти освітньої програми																																
		З1	З2	З3	З4	З5	З6	З7	З8	Б1	Б2	Б3	Б4	Ф1	Ф2	Ф3	Ф4	Ф5	Ф6	Ф7	Ф8	Ф9	Ф10	Ф11	Ф12	Ф13	Ф14	Ф15	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																								*								*	
	РН20																				*	*		*								*	*	
	РН21																	*			*					*					*	*	*	
	РН22								*																									

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 15 травня 2024 р. № 686. Зареєстровано в Міністерстві юстиції України 04 липня 2024 р. за № 1013/42358. [Електронний ресурс]. https://zakon.rada.gov.ua/laws/show/z1013-24#Text.

2. Бутенко А. Роз'яснення щодо застосування Критеріїв оцінювання якості освітньої програми: методичний посібник [Електронне видання] / А. Бутенко, Г. Денискіна, О. Єременко, О. Книш, І. Сімшаг, О. Требенко. – Київ : Національне агентство із забезпечення якості вищої освіти, 2024. – 127 с.

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. Стандарт вищої освіти підготовки бакалавра зі спеціальності 125 Кібербезпека та захист інформації. СВО-2024. – К. : МОН України, 2024. – 18 с. – Затверджено і введено в дію наказом МОН України від 29.10.2024 р. № 1547.

10. 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.

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

12. Положення про організацію освітнього процесу Національного технічного університету «Дніпровська політехніка» / Мін-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2024. – 46 с. Режим доступу: https://surl.li/qgvmos.

13. Положення про формування переліку та обрання навчальних дисциплін

здобувачами вищої освіти Національного технічного університету «Дніпровська політехніка» (зі змінами та доповненнями, затвердженими Вченою радою університету від 22.04.2021, протокол № 7) / Нац. техн. ун-т «Дніпровська політехніка». Дніпро, НТУ «ДП», 2021. – 12 с.

14. Положення про порядок реалізації права на академічну мобільність Національного технічного університету “Дніпровська політехніка” від 19.04.2018 р.

15. Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти / Постанова Кабінету міністрів України від 16 грудня 2022р. № 1392.

16. Наказ Міністерства освіти і науки України «Про внесення змін до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти» від 29.10.2024 р. № 1547.

17. Наказ Міністерства освіти і науки України «Про затвердження Типової програми навчальної дисципліни «Основи національного спротиву»» від 30 червня 2026 р. № 1002.

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 2025 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
Іванькова Марія Сергіївна

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА» БАКАЛАВРА СПЕЦІАЛЬНОСТІ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Електронний ресурс

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

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму «Кібербезпека»
першого (бакалаврського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Динамічність розвитку ІТ-галузі та її стратегічне значення вимагає розвинутої системи захисту інформації, а також реагування на запити ринку праці, зокрема, враховуючи галузевий та регіональний контекст. Останніми роками у місті Дніпро спостерігається стійкий розвиток ІТ-галузі, який продукує потребу у фахівцях з кібербезпеки та захисту інформації. В той же час, на ринку праці регіону спостерігається стійкий дефіцит кваліфікованих кадрів, зокрема фахівців, здатних проводити теоретичні та експериментальні дослідження в галузі кібер- та інформаційного захисту; формулювати та ефективно розв'язувати спеціалізовані завдання практичного характеру відповідного рівня професійної діяльності на основі поєднання освіти, науки та інновацій із забезпеченням інтеграції до міжнародного науково-освітнього простору, що сприяє соціальній стійкості й мобільності випускника на ринку праці.

Зміст ОПП «Кібербезпека» має чітку структуру, освітні компоненти, що включені до неї є логічно викладеними та дозволяють розкрити суть актуальних на сьогодні проблем захисту інформації з урахуванням сучасних реалій ІТ-бізнесу. Наявність вибіркової частини освітніх компонентів дозволяє здобувачам самостійно формувати власну індивідуальну освітню траєкторію та формувати відповідні фахові компетентності.

Вважаю важливим залучення до проведення аудиторних занять професіоналів-практиків з Придніпровського регіонального науково-технічного центру технічного захисту інформації.

Освітньо-професійна програма враховує перспективні напрямки розробок штучного інтелекту, забезпечує глибокі знання щодо сучасних моделей, методів, алгоритмів забезпечення кібербезпеки та захисту інформації, передбачає вивчення сучасних засобів інформаційно-комунікаційних технологій.

З огляду на вищезазначене, вважаю, що рецензована освітньо-професійна програма може бути рекомендована до впровадження в процес підготовки здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації.

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

РЕЦЕНЗІЯ
на освітньо-професійну програму підготовки здобувачів вищої освіти «Кібербезпека» першого (бакалаврського) освітнього рівня за спеціальністю F5 Кібербезпека та захист інформації

Постійний розвиток та рівень впровадження різних інформаційних технологій у всіх сферах життєдіяльності потребує підвищення рівня безпеки та захисту інформації, що має обіг у суспільстві, підприємствах, установах та організаціях різних форм власности. Таким чином, освітньо-професійна програма «Кібербезпека» підготовки бакалаврів зі спеціальності F5 Кібербезпека та захист інформації, що подана на розгляд, є безумовно важливою та актуальною.

Метою даної ОПП є підготовка фахівців, здатних розробляти, використовувати і впроваджувати технології інформаційної та/або кібербезпеки для профілактики інцидентів кібербезпеки і протидії кібератакам в інформаційно-комунікаційних системах та мережах, зокрема, об'єктів критичної інфраструктури.

Подана на рецензію освітньо-професійна програма розроблена на основі стандарту вищої освіти за спеціальністю F5 Кібербезпека та захист інформації для першого (бакалаврського) рівня вищої освіти. Вона передбачає формування загальних та спеціальних компетентностей, що вирішується через навчання та практичну підготовку.

Перелік компонентів ОПП та їх логічна послідовність відповідають розмаїттю вимог роботодавців різних форм власності. Структурно-логічна схема має завершену структуру, що позитивно впливає на якість та рівень засвоєння навчального матеріалу здобувачами вищої освіти.

Програма містить обов'язкові та вибіркові компоненти і передбачає достатню кількість часу на теоретичну і практичну підготовку студентів.

Підсумовуючи, розглянута освітньо-професійна програма «Кібербезпека» підготовки бакалаврів зі спеціальності F5 Кібербезпека та захист інформації Національного технічного університету «Дніпровська політехніка» є своєчасною, перспективною та відповідає всім запитам сучасного світу IT простору. Тому її можна рекомендувати для підготовки здобувачів вищої освіти за першим освітнім рівнем (бакалавр) зі спеціальності F5 Кібербезпека та захист інформації.

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