МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Ректор ВНТУ
_____ Віктор БІЛІЧЕНКО
Наказ ВНТУ № 20 від 26.01.2023 р.

ОСВІТНЬО-НАУКОВА ПРОГРАМА

Кібербезпека
Cyber Security

Рівень вищої освіти	третій (освітньо-науковий)
Спеціальність	125 Кібербезпека та захист інформації
Галузь знань	12 Інформаційні технології
Освітня кваліфікація	доктор філософії з кібербезпеки та захисту інформації

Розглянуто та схвалено
на засіданні Вченої Ради ВНТУ
Протокол №6 від 26.01.2023 р.

Вінниця, 2023

ЛИСТ ПОГОДЖЕННЯ

ОНП Кібербезпека

Рівень вищої освіти третій (освітньо-науковий)
Спеціальність 125 Кібербезпека та захист інформації

Гарант ОНП
д. т. н., проф., зав. кафедри ЗІ _____ Володимир ЛУЖЕЦЬКИЙ

Директор Центру забезпечення
якості освіти ВНТУ _____ Олеся ВОЙТОВИЧ

Освітньо-наукову програму розглянуто та схвалено на засіданні кафедри захисту інформації
Протокол № 6 від 17 грудня 2022 р.

Зав. кафедри ЗІ _____ Володимир ЛУЖЕЦЬКИЙ

ОНП розглянуто після надходження всіх зауважень та пропозицій та схвалено на:

Засіданні секції Науково-технічної ради ВНТУ
протокол №4 від 19 січня 2023 р.
Керівник _____ Андрій КАШКАНОВ

ПРЕАМБУЛА

ОНП Кібербезпека

Рівень вищої освіти	третій (освітньо-науковий)
Спеціальність	125 Кібербезпека та захист інформації

РОЗРОБНИКИ

В. А. Лужецький	Гарант ОНП, завідувач кафедри захисту інформації, д. т. н., проф.
Н. Р. Кондратенко	професор кафедри захисту інформації, к. т. н., професор
Л. М. Куперштейн	доцент кафедри захисту інформації, к. т. н., доцент

Освітньо-професійну програму розглянуто та схвалено на засіданні Наукового товариства студентів та аспірантів

протокол № 2 від 18 січня 2023 р.

Голова _____ Дмитро КУДРЯВЦЕВ

РЕЦЕНЗІЇ-ВІДГУКИ РОБОТОДАВЦІВ

На освітньо-наукову програму надіслали рецензії та відгуки:

Рецензія заступника директора Науково дослідного центру судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції д.т.н. Можаєва М. О.

Рецензія професора спеціальної кафедри №1 Інституту спеціального звязку та захисту інформації Національного технічного університету України КПІ ім. Сікорського д.т.н., професора Іванченка С. О.

Рецензія начальника Департаменту кіберполіції Національної поліції України, доктор філософії Виходець Ю.

1. ПРОФІЛЬ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва ЗВО та структурного підрозділу	Вінницький національний технічний університет, кафедра захисту інформації
Ступінь вищої освіти	Доктор філософії
Освітня кваліфікація	доктор філософії з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – доктор філософії. Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – Кібербезпека
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом доктора філософії (PhD), обсяг освітньої складової 50 кредитів ЄКТС, термін навчання – 4 роки
Цикл / рівень	НРК України – 8 рівень, EQF-LLL – 8 рівень, QF-EHEA – третій цикл
Наявність акредитації	--
Передумови	Для здобуття освітньо-наукового ступеня доктора філософії можуть вступати особи, що здобули освітній ступінь магістра (освітньо-кваліфікаційний рівень спеціаліста). Програма фахових вступних випробувань повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека для другого (магістерського) рівня вищої освіти.
Мови викладання	Українська, за потреби декілька або всі освітні компоненти можуть викладатись англійською мовою
Інтернет-адреса постійного розміщення опису освітньої програми	https://vntu.edu.ua/uk/information-for-enrollee/progmagbak.html
2 – Мета освітньо-наукової програми	
Підготовка висококваліфікованих, конкурентоспроможних, інтегрованих у Європейський та світовий науково-освітній простір фахівців, здатних до самостійної науково-дослідницької, науково-організаційної, педагогічної та практичної діяльності в галузі кібербезпеки та захисту інформації завдяки знанням та досвіду викладачів та у співпраці з ними для задоволення потреб суспільства і держави у фахівцях, які забезпечують підвищення рівня захищеності інформаційних ресурсів Вінниччини та інших регіонів України та світу.	
3 – Характеристика освітньо-наукової програми	
Опис предметної області	**Об’єкт діяльності**: інноваційні підходи та технології кібербезпеки та захисту інформації, що циркулює в інформаційно-комунікаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури. **Цілі навчання**: набуття здатності розв’язувати комплексні проблеми професійної та/або дослідницько-інноваційної

	діяльності у галузі кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики. **Теоретичний зміст предметної області**: фундаментальні та прикладні науково-дослідні роботи, аналіз, проєктування, інноваційні підходи до вирішення комплексних проблем у галузі кібербезпеки та захисту інформації; методи дослідження систем, процесів та технологій кібербезпеки та захисту інформації на різних рівнях.
Орієнтація освітньої програми	Освітньо-наукова
Методи, методики та технології	Загальнонаукові методи пізнання та дослідницької діяльності; методи математичного аналізу, моделювання та синтезу систем і об'єктів; методики і технології визначення та аналізу ризиків інформаційної і кібербезпеки; методи, моделі та засоби кібербезпеки та захисту інформації; інформаційно-комунікаційні технології презентації результатів досліджень; методи та методики викладацької діяльності.
Інструменти та обладнання	засоби, прилади та комплекси для моделювання об'єктів та систем; програмні, апаратні та програмно-апаратні комплекси, що використовуються для вирішення задач кібербезпеки та захисту інформації об'єктів інформаційної діяльності; комп'ютеризовані системи у навчальній та викладацький діяльності.
Основний фокус освітньої програми	Формування фахівців, які володіють дослідницькими навиками для наукової та професійної діяльності, комерціалізації результатів дослідницької діяльності, викладання спеціальних дисциплін у галузі інформаційної та кібербезпеки, зокрема, безпеки інформаційно-комунікаційних технологій і систем та на об'єктах інформаційної діяльності.
Особливості програми	Програма забезпечує ґрунтовну дослідницьку підготовку, в основі якої лежить використання сучасних методів та засобів інформаційної безпеки та кібербезпеки для вирішення задач, що виникають у соціотехнічних системах, зокрема на інформаційних об'єктах критичної інфраструктури. Здобувачі вищої освіти працюють під науковим керівництвом досвідчених науковців, які проводять та публікують дослідження за такими напрямами. 1. Криптографічний захист інформації. Розвиток псевдонедетермінованого підходу до криптографічного захисту інформації, розробка моделей методів і засобів криптографічних перетворень малоресурсної криптографії, криптографія на основі квазігруп. 2. Інтелектуальні системи прийняття рішень у кібербезпеці. Детектування вузлів інформаційно-комунікаційних мереж на

	базі методів машинного навчання, класифікація об'єктів в кібербезпеці, захист пірингових мереж, розробка моделей безпеки для об'єктів критичної інфраструктури. Детектування атак на відмову в обслуговуванні. 3. Методи та засоби підтримки прийняття рішень в задачах кібербезпеки. Моделі інформаційної безпеки та кібербезпеки соціотехнічних систем, побудова моделей та ідентифікація загроз та атак в соціотехнічних системах, виявлення фейкових повідомлень та облікових записів, проведення досліджень інцидентів інформаційної та кібербезпеки, методи та засоби моніторингу та аудиту інформаційної безпеки та кібербезпеки. Проєктування систем захисту інформації.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до класифікатора професій ДК 003:2010, затвердженого Наказом Держспоживстандарту України від 28.07.2010 за № 327 та враховуючи реальні потреби ринку праці доктори філософії зі спеціальності 125 «Кібербезпека» мають такі перспективи працевлаштування: - Викладачі університету та вищого навчального закладу (код 2310). - Наукові співробітники науково-дослідницької, виробничої установи (код 2139.1). - Наукові співробітники-консультанти науково-дослідницької, виробничої установи (код 2139.1). - Професіонали із організації інформаційної безпеки (код 2149).
Подальше навчання	Здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих
5 – Викладання та оцінювання	
Викладання та навчання	Лекційні та практичні заняття, консультації, робота з науковою літературою, педагогічна практика, виступи на конференціях, написання наукових праць та оформлення дисертації.
Оцінювання	Письмові та усні заліки, поточне оцінювання (тестування, виконання практичних робіт, есеїв, презентацій, індивідуальних дослідницьких завдань), презентація власних наукових досягнень.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у галузі кібербезпеки, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.
Загальні компетентності	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність до пошуку, оброблення та аналізу

	інформації з різних джерел. ЗК3. Здатність працювати в міжнародному контексті. ЗК4. Здатність розв'язувати комплексні проблеми кібербезпеки та захисту інформації на основі системного наукового світогляду та загального культурного кругозору з дотриманням принципів професійної етики та академічної доброчесності.
Фахові (спеціальні) компетентності [1]	ФК1. Здатність планувати та виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у інформаційній безпеці та кібербезпеці та дотичних до неї міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з відповідних галузей. ФК2. Здатність усно і письмово презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок в кібербезпеці та захисті інформації українською та англійською мовами, глибоке розуміння англомовних наукових текстів за напрямом наукових досліджень. ФК3. Здатність застосовувати нові технології та інструменти, сучасні цифрові технології, спеціалізоване програмне та апаратне забезпечення у науковій та навчальній діяльності. ФК4. Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проєкти в сфері кібербезпеки та захисту інформації та дотичні до неї міждисциплінарні проекти, лідерство під час їх реалізації. ФК5. Здатність обґрунтовувати та захищати методологію та результати досліджень і проєкти у галузі кібербезпеки та захисту інформації. ФК6. Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері кібербезпеки та захисту інформації, оцінювати та забезпечувати якість виконуваних досліджень. ФК7. Здатність здійснювати науково-педагогічну діяльність у вищій освіті. ФК8. Здатність створювати та аналізувати математичні моделі об'єктів, процесів та явищ; використовувати інструменти математичного моделювання в дослідницькій діяльності. ФК9. Здатність забезпечувати проєктування, розроблення та технічний супровід систем кібербезпеки та захисту інформації.
7 – Програмні результати навчання	
ПРН1. Мати передові концептуальні та методологічні знання у сфері кібербезпеки та захисту інформації і на межі галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні світових досягнень з кібербезпеки, отримання нових знань та здійснення інновацій. ПРН2. Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосувати їх у власних	

дослідженнях у сфері кібербезпеки та захисту інформації, а також у викладацькій практиці. ПРН3. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні джерела ПРН4. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно їх використовувати для отримання нових знань та/або створення інноваційних продуктів у кібербезпеці та дотичних міждисциплінарних напрямах. [1] ПРН5. Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації, а також дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. ПРН6. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи. ПРН7. Розробляти та реалізовувати наукові та/або інноваційні інженерні проєкти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми кібербезпеки та захисту інформації з врахуванням соціальних, економічних, екологічних та правових аспектів. ПРН8. Досліджувати, проєктувати, розробляти, застосовувати, вдосконалювати та впроваджувати наукові та інженерні рішення, засоби, методи та технології для вирішення проблем кібербезпеки та захисту інформації. ПРН9. Вирішувати комплексні проблеми кібербезпеки та захисту інформації для створення систем захисту інформації за допомогою сучасних технологій. ПРН10. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях. ПРН11. Складати пропозиції щодо міжнародного наукового співробітництва, а також щодо фінансування наукових досліджень у сфері кібербезпеки та захисту інформації. ПРН12. Організовувати і здійснювати освітній процес у галузі кібербезпеки та захисту інформації, наукове, навчально-методичне та нормативне забезпечення, застосувати ефективні методики викладання навчальних дисциплін. ПРН13. Досліджувати, розробляти, застосовувати та вдосконалювати фундаментальні методи і прикладні інструменти з кібербезпеки та захисту інформації.
8 – Ресурсне забезпечення реалізації програми

Кадрове забезпечення	Кадрове забезпечення ОНП формується в основному за рахунок кафедри захисту інформації. До викладання дисциплін залучаються також провідні викладачі інших кафедр університету. Гарант, наукові керівники та викладацький склад, який забезпечує реалізацію ОНП, відповідають вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності. Всі викладачі мають наукові ступені та вчені звання.

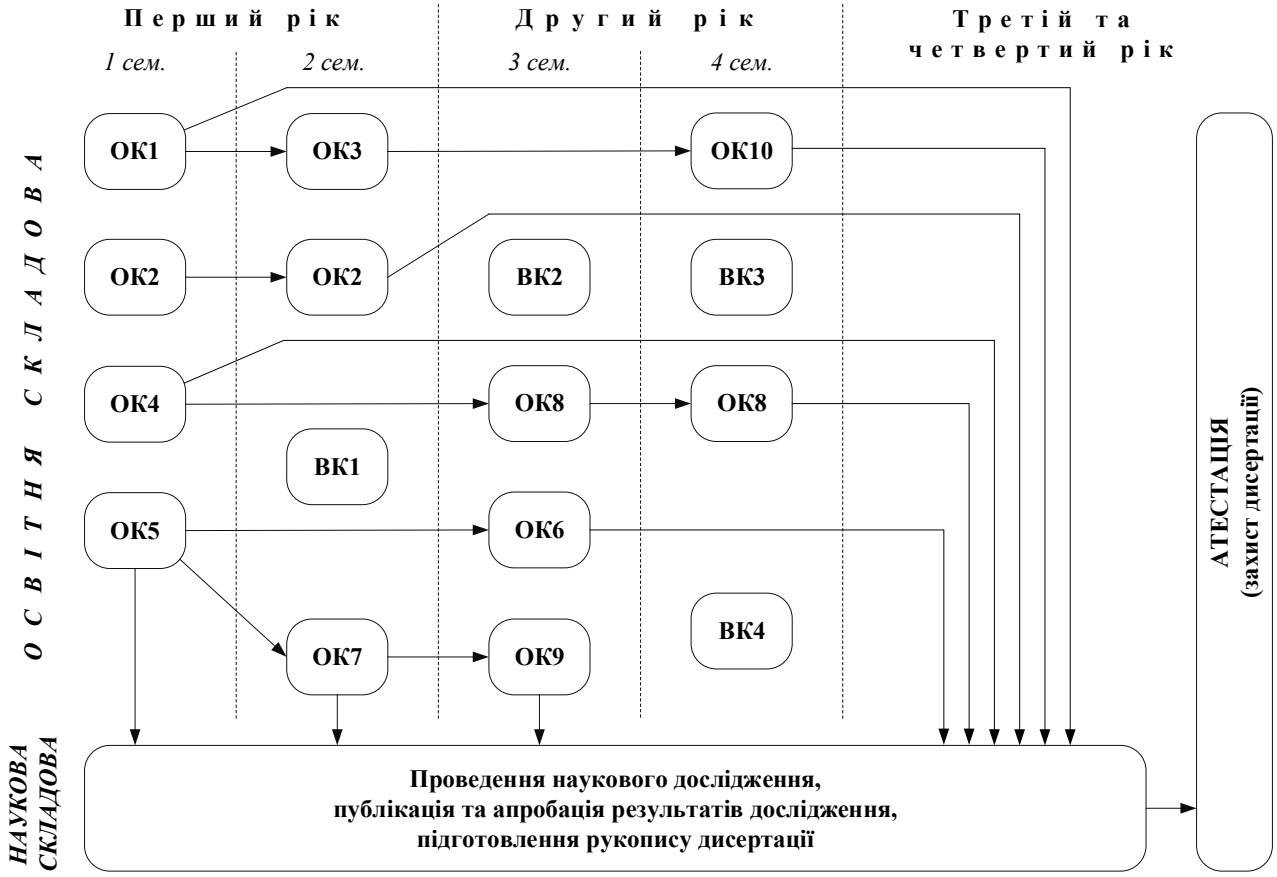
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності, в тому числі включає спеціалізовані лабораторії (лабораторію захисту програмного забезпечення, лабораторію технічного захисту інформації, лабораторію захисту комп'ютерних мереж), спрямовані на здобуття компетентностей, та результатами навчання в галузі кібербезпеки та захисту інформації. Здобувачі освіти забезпечені гуртожитком. Наявна соціально-побутова та спортивна інфраструктура.
Інформаційне та навчально-методичне забезпечення	Відповідно до вимог Ліцензійних умов провадження освітньої діяльності включає ресурси науково-технічної бібліотеки, репозиторій університету, електронні навчальні ресурси, веб-сайт ВНТУ та кафедри, інформаційну систему підтримки освітнього процесу JetIQ, на яких розміщена інформація щодо змісту й організації освітньої діяльності за ОНП. Університет надає доступ до мережі Wi-Fi та Інтернет, постійно вдосконалюється інформаційна система JetIQ, забезпечено доступ до міжнародних наукометричних баз даних Scopus, Web of Science Core Collection та інших баз наукової інформації, регулярно організовуються тематичні семінари та вебінари.
9 – Академічна мобільність	
Національна кредитна мобільність	Здійснюється на підставі укладених угод про співробітництво між ВНТУ та ЗВО України.
Міжнародна кредитна мобільність	Здійснюється на підставі укладених угод між ВНТУ та освітніми установами країн-партнерів за узгодженими та затвердженими індивідуальними навчальними планами здобувачів освіти та програмами навчальних дисциплін, а також інших угод щодо міжнародної академічної мобільності.
Навчання іноземних здобувачів вищої освіти	Передбачено

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ СКЛАДОВОЇ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ

Код ОК	Компоненти ОНП	Кількість кредитів	Форма контролю
Обов'язкові компоненти			
Освітні компоненти загальнонаукового (філософського) спрямування			
ОК1	Філософсько-світоглядні засади сучасної науки й цивілізації	3	диф. залік
Освітні компоненти мовного спрямування			
ОК2	Іноземна мова наукового спрямування Українська мова як іноземна*	6	диф. залік
Освітні компоненти формування педагогічних навичок			
ОК3	Сучасні педагогічні технології у закладах вищої освіти	3	диф. залік
Освітні компоненти формування універсальних навичок дослідника			
ОК4	Математичне моделювання в наукових дослідженнях	3	диф. залік
Освітні компоненти спеціального спрямування			
ОК5	Організація та планування експериментальних досліджень в інформаційній та кібербезпеці	3	диф. залік
ОК6	Наукові засади технічного захисту інформації	3	диф. залік
ОК7	Алгебраїчні структури і математичні алгоритми криптографії	4	диф. залік
ОК8	Наукові засади захисту інформації у кіберпросторі	6	диф. залік
ОК9	Наукові засади управління інформаційною безпекою	3	диф. залік
Практики			
ОК10	Педагогічна практика	3	диф. залік
Загальний обсяг обов'язкових компонентів		37 кредитів ЄКТС	
Вибіркові компоненти			
ВК1	Дисципліна 1	3	залік
ВК2	Дисципліна 2	3	залік
ВК3	Дисципліна 3	3	залік
ВК4	Дисципліна 4	4	залік
Загальний обсяг вибіркових компонентів		13 кредитів ЄКТС	
Загальний обсяг освітньої складової ОНП		50 кредитів ЄКТС	

* для іноземних здобувачів освіти

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ



4. НАУКОВА СКЛАДОВА ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ ТА ФОРМА ВИПУСКНОЇ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Наукова складова освітньо-наукової програми передбачає проведення власного наукового дослідження під керівництвом одного або двох наукових керівників та оформлення його результатів у вигляді дисертації. Напрями досліджень наукового керівника (керівників) повинні відповідати науковим інтересам здобувача вищої освіти рівня доктора філософії.

Обов’язковою умовою допуску до захисту дисертації є успішне виконання аспірантом його індивідуального навчального плану.

Атестація здобувачів ступеня доктора філософії здійснюється у формі публічного захисту дисертаційної роботи.

Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що містить результати розв’язання комплексної проблеми в сфері кібербезпеки та захисту інформації, або на її межі з іншими спеціальностями, результати якого мають наукову новизну, теоретичне та практичне значення.

Дисертаційна робота не повинна містити академічного плагіату, фальсифікації, фабрикації.

Дисертаційна робота повинна бути розміщена на сайті закладу вищої освіти або його структурного підрозділу.

Дисертаційна робота має відповідати іншим вимогам, встановленим чинним законодавством.

7. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

У ВНТУ функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ВНТУ, на інформаційних стендах або в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників і здобувачів вищої освіти;

9) інших процедур і заходів.

Система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням ЗВО оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним агентством із забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

8. ПЕРЕЛІК НОРМАТИВНИХ ДОКУМЕНТІВ, НА ЯКИХ БАЗУЄТЬСЯ ОСВІТНЬО-НАУКОВА ПРОГРАМА

- Стандарт вищої освіти третього (освітньо-наукового) рівня, ступеня доктора філософії, галузі знань 16 Хімічна на біоінженерія, спеціальності 163 Біомедична інженерія, Київ, 2021. https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzheni.Standarty/01/11/163-Biomed.inzhener-Doktor.filosofiyi-VO-zatv.stand.01.11.pdf
- Закон України від 01.07.2014 № 1556-VII «Про вищу освіту»;

− Постанова Кабінету Міністрів України від 23.11.2011 р. № 1341 «Про затвердження національної рамки кваліфікацій»;
− Постанова Кабінету Міністрів України від 29.04.15 року № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»;
− Класифікація видів економічної діяльності : ДК 009:2010. – На заміну ДК 009:2005 ; Чинний від 2012-01-01. – (Національний класифікатор України);
− Національна рамка кваліфікацій. Затверджена Постановою КМУ № 1341 від 23 листопада 2011 р. (зі змінами, внесеними згідно з Постановою КМУ № 509 від 12 червня 2019 р.). – https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF/ed20190625#Text;
− Методичні рекомендації щодо розроблення стандартів вищої освіти. Схвалено сектором вищої освіти Науково-методичної Ради Міністерства освіти і науки України протокол від 29 березня 2016 року, № 3. – http://mon.gov.ua/content/Діяльність/Реформаосвіти/07-metod-rekomendacziyi.doc;
− Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти. – К. : Ленвіт, 2006. – 35 с. ISBN 966-7043-96-7;
− Національний освітній глосарій: вища освіта / 2-е вид., перероб. і доп. / авт.-уклад. : В. М. Захарченко та ін. / За ред. В. Г. Кременя. – К. : ТОВ «Видавничий дім «Плеяди», 2014. – 100 с. ISBN 978-966-2432-22-0.
− Міжнародна Стандартна Класифікація Освіти (ISCED-97: International Standard Classification of Education/UNESCO, Paris);
− Структури кваліфікацій для Європейського простору вищої освіти (The framework of qualifications for the European Higher Education Area);
− Структури ключових компетенцій, які розглядаються як необхідні для всіх у суспільстві, заснованому на знаннях (Key Competences for Lifelong learning: A European Reference Framework - IMPLEMENTATION OF "EDUCATION AND TRAINING 2010", Workprogram, WorkingGroup B "KeyCompetences", 2004.);
− Національний класифікатор України ДК 009:2010 "Класифікація видів економічної діяльності". К.: Центр учбової літератури, 2011 р., 224 с.;
− Національний класифікатор професій ДК 003:2010. - К.: Держспоживстандарт України, - 2010. – 697 с.;
− Довідник кваліфікаційних характеристик професій працівників. Галузеві випуски. - Краматорськ: Видавництво центру продуктивності.
− Положення про розроблення і супроводження освітніх програм. – Вінниця : ВНТУ, 2020. – https://vntu.edu.ua/uploads/2020/polsv.pdf

Пояснювальна записка

Освітньо-наукова програма містить програмні компетентності, що визначають специфіку підготовки докторів філософії зі спеціальності 125 Кібербезпека та захист інформації у ВНТУ та програмні результати навчання, які виражають те, що здобувач освіти повинен знати, розуміти та бути здатним виконувати після успішного завершення освітньої програми. В таблицях 1, 2 наведені матриці відповідності визначених освітньою програмою відповідно компетентностей і програмних результатів навчання та освітніх компонентів.

Таблиця 1. Матриця відповідності компетентностей компонентам освітньо-наукової програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10
ЗК1	+			+						+
ЗК2	+	+								+
ЗК3	+	+	+			+			+	
ЗК4	+		+							+
ФК1				+	+	+	+	+	+	
ФК2		+	+						+	+
ФК3							+	+		+
ФК4			+					+	+	+
ФК5					+		+			+
ФК6						+	+		+	
ФК7	+		+		+					+
ФК8				+				+		
ФК9					+	+		+		
ІК*	+	+	+	+	+	+	+	+	+	+

Таблиця 2. Матриця забезпечення програмних результатів навчання компонентами освітньо-наукової програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10
ПРН1				+	+	+	+	+	+	
ПРН2			+	+	+	+	+	+	+	+
ПРН3	+	+		+		+		+	+	+
ПРН4				+				+		
ПРН5	+				+	+			+	+
ПРН6				+			+	+		+
ПРН7	+		+		+		+		+	
ПРН8					+	+	+	+	+	
ПРН9						+	+	+	+	
ПРН10		+			+					+
ПРН11		+	+		+	+	+	+	+	+
ПРН12	+		+		+		+	+		+
ПРН13							+		+	

АРКУШ РЕЄСТРАЦІЇ ЗМІН

Номер зміни	Введено в дію	Що змінено	Коли набуває чинності