МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Ректор ВНТУ
_____ Віктор БІЛІЧЕНКО
Наказ ВНТУ № 105 від 27.03.2025

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Етичний хакінг і кібербезпека

Ethical Hacking and Cybersecurity

Рівень вищої освіти	перший (бакалаврський)
Спеціальність	F5 Кібербезпека та захист інформації
Галузь знань	F Інформаційні технології
Освітня кваліфікація	бакалавр з кібербезпеки та захисту інформації

Розглянуто та схвалено
на засіданні Вченої Ради ВНТУ
Протокол № 10 від 27.03.2025

Вінниця, 2025

ЛИСТ ПОГОДЖЕННЯ

ОПП Етичний хакінг і кібербезпека

Рівень вищої освіти перший (бакалаврський)

Спеціальність F5 Кібербезпека та захист інформації

Гарант ОПП

к. т. н., доцент, доцент кафедри ЗІ _____ Юрій БАРИШЕВ

Директор Центру забезпечення

якості освіти ВНТУ _____ Станіслав ТУЖАНСЬКИЙ

Освітньо-професійну програму розглянуто та схвалено на засіданні кафедри захисту інформації;

протокол № 12 від 11.02.2025

Зав. кафедри _____ Володимир ЛУЖЕЦЬКИЙ

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

засіданні Вченої ради факультету інформаційних технологій та комп'ютерної інженерії;

протокол №7 від 18.03.2025

Голова _____ Світлана КИРИЛАЩУК

засіданні Ради з якості освіти ВНТУ,

протокол №8 від 20.03.2025

Голова _____ Олександр ПЕТРОВ

ПРЕАМБУЛА

ОПП Етичний хакінг і кібербезпека

Рівень вищої освіти перший (бакалаврський)

Спеціальність F5 Кібербезпека та захист інформації

Освітньо-професійна програма (далі – ОПП) підготовки бакалаврів зі спеціальністю 125 Кібербезпека та захист інформації розроблена на основі стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти затвердженого Наказом МОН України №1547 від 29.10.24.

РОЗРОБНИКИ

Гарант ОПП, доцент кафедри захисту інформації, к. т. н., доцент	Юрій БАРИШЕВ
завідувач кафедри захисту інформації, д. т. н., професор	Володимир ЛУЖЕЦЬКИЙ
доцент кафедри захисту інформації, к. т. н., доцент	Олеся ВОЙТОВИЧ
доцент кафедри захисту інформації, к. т. н., доцент	Володимир ГАРНАГА

Освітньо-професійну програму розглянуто та схвалено на засіданні Студентської ради факультету інформаційних технологій та комп'ютерної інженерії;

протокол № 21 від 17.03.2025

Голова Софія БАБЕНКО

РЕЦЕНЗІЇ-ВІДГУКИ РОБОТОДАВЦІВ

На освітньо-професійну програму надіслали рецензії та відгуки:

Вадим Груша, директор ТОВ Трасті Глобал

Володимир Тітомир, полковник поліції, начальник Управління протидії кіберзлочинам у Вінницькій області

Оксана Білоконь, директор ТОВ ЕлефантсЛаб

1 ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Вінницький національний технічний університет, кафедра захисту інформації
Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти та назва освітньої кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки та захисту інформації
Назва галузі знань	F Інформаційні технології
Назва спеціальності	F5 Кібербезпека та захист інформації
Офіційна назва освітньої програми	Етичний хакінг і кібербезпека
Форма здобуття освіти	Денна
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний 240 кредитів ЄКТС, термін навчання – 3 роки 10 місяців.
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – Етичний хакінг і кібербезпека
Цикл/рівень	6 рівень НРК України, перший цикл FQ-EHEA, 6 рівень EQF-LLL
Передумови	Повна загальна середня освіта
Мова (и) викладання	Українська, за потреби один або декілька освітніх компонентів можуть викладатися англійською мовою
Акредитація	-
Інтернет-адреса постійного розміщення опису освітньої програми	https://jetiq.vntu.edu.ua/edu_progs/ep_list.php
2 – Мета освітньої програми	
Підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації; формування творчої особистості нового покоління, здатної успішно реалізовувати набуті сучасні професійні компетентності з етичного хакінгу і кібербезпеки, інтелектуальний потенціал, навички практичного досвіду та інноваційної діяльності в галузі кібербезпеки та захисту інформації, а також соціально-патріотичні та морально-етичні цінності у глобальному суспільно-економічному просторі	
3 – Характеристика освітньої програми	
Опис предметної області	**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'язання 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).
Особливості програми	ОПП спрямована на забезпечення кібербезпеки та захисту інформації на основі виявлення вразливостей операційних процесів інформаційних систем та програмного забезпечення підприємств та організацій різних форм власності.
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 Кібербезпека та захист інформації та спорідненої з нею.Права випускників на працевлаштування не обмежуються.
Подальше навчання	Мають право продовжити навчання на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсової роботи, лабораторні роботи, самостійна робота на основі навчальних посібників, конспектів лекцій, електронних джерел, консультації із викладачами, семінари, елементи дистанційного навчання, проходження

	практики на профільних підприємствах чи структурних відділах, в науково-дослідних установах, підготовка кваліфікаційної роботи.
Оцінювання	Семестровий контроль: екзамени, заліки, захисти курсових робіт і проєктів, захист звіту з практики. Поточний контроль: захист лабораторних і практичних робіт, тестування, презентації, звіти, модульні контрольні роботи, аналіз текстів або даних тощо.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК 4. Здатність спілкуватись іноземною мовою. ЗК 5. Здатність вчитися і оволодівати сучасними знаннями. ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина України. ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК 8. 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.
Спеціальні (фахові, предметні) компетентності	СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності. СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних

	системах згідно встановленої політики кібербезпеки та захисту інформації. СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційної та кібербезпекою. СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. СК 11. Здатність проводити дослідження програмного забезпечення та систем забезпечення кібербезпеки. СК 12. Здатність проводити тестування на проникнення з метою виявлення та оцінювання вразливостей операційних процесів інформаційних систем та програмного забезпечення щодо відповідності вимогам, що висуваються до них.
7 – Програмні результати навчання	
РН 01. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН 02. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН 03. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН 04. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН 05. 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. РН 06. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. РН 07. 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.
РН 08. 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.
РН 09. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації.
РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
РН 13. 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.
РН 14. 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 та відновлення інформації.
РН 15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН 17. Забезпечувати функціонування систем управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.
РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН 20. 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.
РН 21. 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. РН 22. Виконувати дослідження стійкості до зламу програмного забезпечення та систем забезпечення кібербезпеки, формувати обґрунтовані оцінки за результатами цього дослідження. РН 23. Формувати рекомендації щодо покращення кібербезпеки програмного забезпечення та систем забезпечення кібербезпеки відповідно до результатів кібердосліджень. РН 24. Виконувати тестування на проникнення операційних процесів інформаційних систем та програмного забезпечення з метою встановлення відповідності вимогам, що висуваються до них, та формувати звіт за результатами тестування на проникнення. РН 25. Керуватись законодавчими та етичними нормами під час виконання професійних завдань.	
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення ОПП формується, в основному за рахунок кафедри захисту інформації. До викладання дисциплін залучаються також інші кафедри університету, зокрема менеджменту та безпеки інформаційних систем. Група забезпечення та гарант освітньої програми, які забезпечують її реалізацію, відповідають вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності та іншим нормативним документам.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності, в тому числі включає в себе спеціалізовані лабораторії (захисту програмного забезпечення, технічного захисту інформації, захисту комп'ютерних мереж), направлені на здобуття спеціальних (фахових) компетентностей, оволодіння практичним навичками забезпечення кібербезпеки, зокрема етичного хакінгу, а також інші спеціалізовані лабораторії ВНТУ
Інформаційне та навчально-методичне забезпечення	Включає в себе бібліотечні ресурси, систему підтримки освітнього процесу JetIQ, електронні навчальні ресурси, сайт ВНТУ та сайт кафедри, на яких розміщена основна інформація щодо освітньої діяльності за ОПП.
9 – Академічна мобільність	
Національна кредитна мобільність	Здійснюється на підставі укладення угод про співробітництво між ВНТУ та закладами вищої освіти України.
Міжнародна кредитна мобільність	Здійснюється на підставі укладення угод та меморандумів між ВНТУ та закладами вищої освіти різних країн за узгодженими та затвердженими у встановленому порядку індивідуальними навчальними планами здобувачів вищої освіим та програмами навчальних дисциплін, а також в рамках міжурядових угод про співробітництво в галузі освіти, міжнародних проектів, в яких ВНТУ приймає участь, грантів та ін.

Навчання іноземних здобувачів вищої освіти	За даною освітньою програмою не передбачено навчання іноземних здобувачів вищої освіти

2 ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонентів освітньо-професійної програми

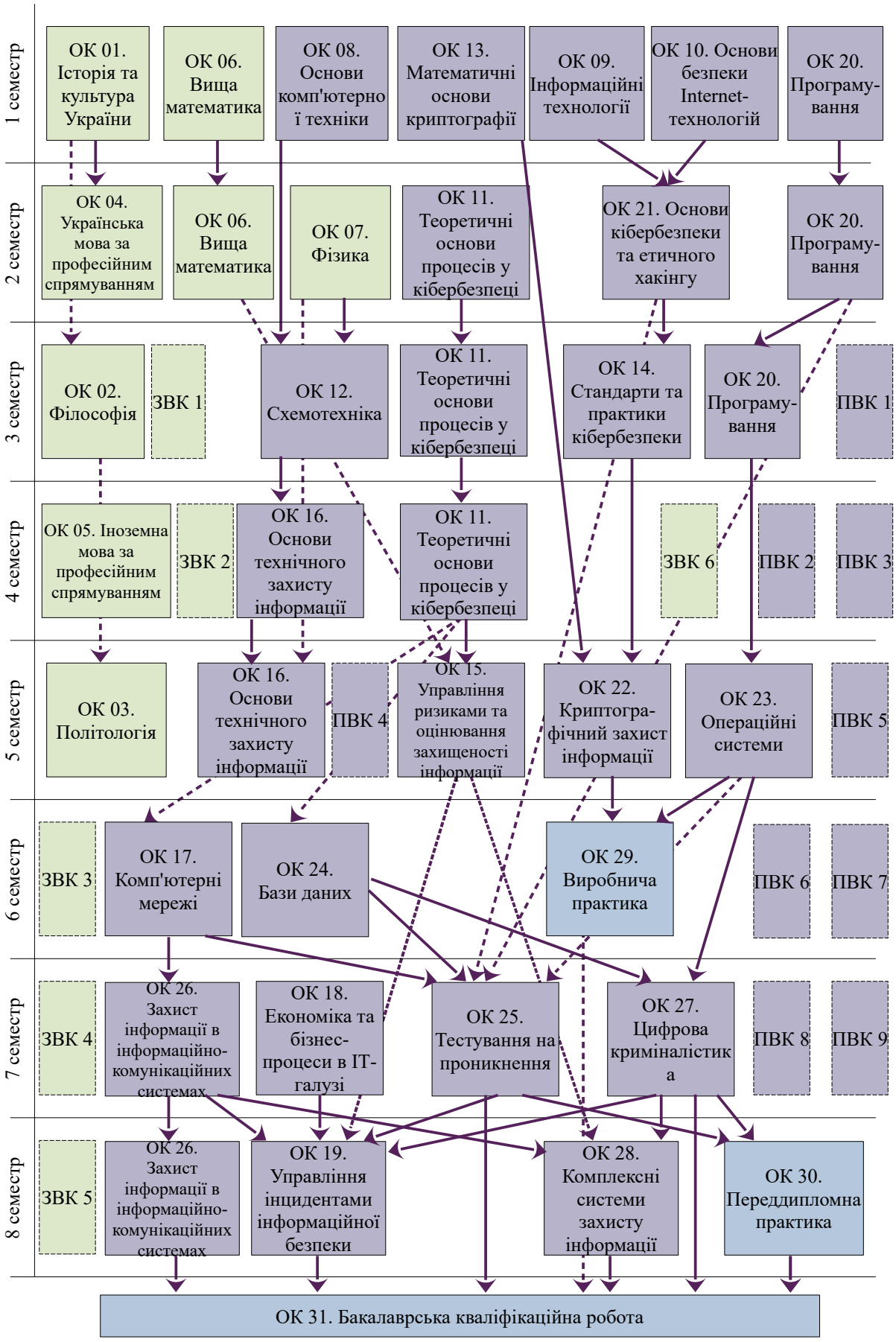
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов’язкові компоненти ОП			
Загальні			
ОК 01.	Історія та культура України	3,0	залік
ОК 02.	Філософія	3,0	залік
ОК 03.	Політологія	3,0	залік
ОК 04.	Українська мова за професійним спрямуванням	3,0	залік
ОК 05.	Іноземна мова за професійним спрямуванням	8,0	залік
ОК 06.	Вища математика	12,0	іспит
ОК 07.	Фізика	5,0	іспит
Професійні			
ОК 08.	Основи комп'ютерної техніки	3,0	іспит
ОК 09.	Інформаційні технології	3,0	залік
ОК 10.	Основи безпеки Internet-технологій	4,0	іспит
ОК 11.	Теоретичні основи процесів у кібербезпеці	12,0	іспит
ОК 12.	Схемотехніка	4,0	залік
ОК 13.	Математичні основи криптографії	4,0	іспит
ОК 14.	Стандарти та практики кібербезпеки	4,0	залік
ОК 15.	Управління ризиками та оцінювання захищеності інформації	7,0	іспит
ОК 16.	Основи технічного захисту інформації	8,0	іспит
ОК 17.	Комп'ютерні мережі	5,0	іспит
ОК 18.	Економіка та бізнес-процеси в ІТ-галузі	3,0	залік
ОК 19.	Управління інцидентами інформаційної безпеки	3,0	іспит
ОК 20.	Програмування	16,0	іспит
ОК 21.	Основи кібербезпеки та етичного хакінгу	3,0	іспит
ОК 22.	Криптографічний захист інформації	6,0	іспит
ОК 23.	Операційні системи	5,0	іспит
ОК 24.	Бази даних	3,0	іспит
ОК 25.	Тестування на проникнення	5,0	іспит
ОК 26.	Захист інформації в інформаційно-комунікаційних системах	9,0	іспит
ОК 27.	Цифрова криміналістика	4,0	іспит
ОК 28.	Комплексні системи захисту інформації	5,0	іспит
ОК 29.	Виробнича практика	9,0	залік
ОК 30.	Переддипломна практика	4,5	залік
ОК 31.	Бакалаврська кваліфікаційна робота	10,5	захист
Загальний обсяг обов’язкових компонентів:		**177**	
2. ВИБІРКОВІ КОМПОНЕНТИ ОП ЗА ВІЛЬНИМ ВИБОРОМ СТУДЕНТА			

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Загальні			
ЗВК 1.	Освітній компонент 1 з БЗДВВ	3,0	залік
ЗВК 2.	Освітній компонент 2 з БЗДВВ	3,0	залік
ЗВК 3.	Освітній компонент 3 з БЗДВВ	3,0	залік
ЗВК 4.	Освітній компонент 4 з БЗДВВ	3,0	залік
ЗВК 5.	Освітній компонент 5 з БЗДВВ	3,0	залік
ЗВК 6.	Освітній компонент 6 з БЗДВВ**	3,0	залік
Професійні			
ПВК 1	Освітній компонент 1 з БПДВВ	5,0	залік
ПВК 2	Освітній компонент 2 з БПДВВ	5,0	залік
ПВК 3	Освітній компонент 3 з БПДВВ	5,0	залік
ПВК 4	Освітній компонент 4 з БПДВВ	5,0	залік
ПВК 5	Освітній компонент 5 з БПДВВ	5,0	залік
ПВК 6	Освітній компонент 6 з БПДВВ	5,0	залік
ПВК 7	Освітній компонент 7 з БПДВВ	5,0	залік
ПВК 8	Освітній компонент 8 з БПДВВ	5,0	залік
ПВК 9	Освітній компонент 9 з БПДВВ	5,0	залік
Загальний обсяг вибіркових компонентів:		**63**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	
ЗВК 6.	Теоретична підготовка базової загальновійськової підготовки*	3,0	
	Практична підготовка базової загальновійськової підготовки*	7,0	

* - є обовязковими відповідно до Закону України про військовий обов'язок і військову службу та вивчається у Порядку затвердженому Постановою КМУ №734 від 21.06.2024 р.

** - вибирається особами, що не підпадають під вимоги Закону України про військовий обов'язок і військову службу та Порядку затвердженому Постановою КМУ №734 від 21.06.2024 р.

2.2. Структурно-логічна схема освітньо-професійної програми



3 ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти

Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.

Вимоги єдиного державного кваліфікаційного іспиту

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених Стандартом.

Вимоги до кваліфікаційної роботи

Кваліфікаційна робота має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації.

У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації.

Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті ВНТУ (репозитарії) у системі JetIQ.

4 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 ВНТУ та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті ВНТУ;
4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;
5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів вищої освіти, 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 ВНТУ і здобувачів вищої освіти;
9) інших процедур і заходів, які забезпечують належний рівень якості вищої освіти.

Система забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням ВНТУ 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.

5 ПЕРЕЛІК НОРМАТИВНИХ ДОКУМЕНТІВ, НА ЯКИХ БАЗУЄТЬСЯ ОСВІТНЯ ПРОГРАМА

1. Про вищу освіту: Закон України URL: http://zakon4.rada.gov.ua/laws/show/1556-18.
2. Про освіту: Закон України URL: https://zakon.rada.gov.ua/laws/show/2145-19
3. Про захист персональних даних: Закон України URL: https://zakon.rada.gov.ua/laws/show/2297-17
4. Про доступ до публічної інформації: Закон України URL: https://zakon.rada.gov.ua/laws/show/2939-17
5. Про основні засади забезпечення кібербезпеки України: Закон України URL: https://zakon.rada.gov.ua/laws/show/2163-19
6. Про захист інформації в інформаційно-комунікаційних системах : Закон України URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
7. Про державну таємницю: Закон України URL: https://zakon.rada.gov.ua/laws/show/3855-12
8. Про науково-технічну інформацію: Закон України URL: https://zakon.rada.gov.ua/laws/show/3322-12
9. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF
10. Національний класифікатор України. Класифікатор професій ДК 003:2010 URL: https://zakon.rada.gov.ua/rada/show/va327609-10
11. Про затвердження національної рамки кваліфікацій: Постанова Кабінету Міністрів України від 23 листопада 2011 р. № 1341. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF
12. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти: Постанова Кабінету Міністрів України від 29 квітня 2015 р. № 266. URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF
13. Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти: Постанова Кабінету Міністрів України від 30 серпня 2024 р. № 1021. URL: https://zakon.rada.gov.ua/laws/show/1021-2024-%D0%BF

ПОЯСНЮВАЛЬНА ЗАПИСКА

Освітньо-професійна програма містить програмні компетентності, що визначають специфіку підготовки бакалаврів зі спеціальності F5 Кібербезпека та захист інформації, а також програмні результати навчання, які відображають те, що здобувач вищої освіти повинен знати, розуміти та бути здатним виконувати після успішного завершення освітньої програми. В таблицях 1, 2 Додатку Б наведені матриці відповідності визначених освітньою програмою результатів навчання (компетентностей) та освітніх компонентів.

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Концептуальні наукові та практичні знання **Зн2** Критичне осмислення теорій, принципів, методів і понять	**Уміння** **Ум1.** Поглиблені когнітивні та практичні уміння/навички для вирішення складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання	**Комунікація** **К1** — донесення до фахівців інформації, ідей, рішень та аргументації **К2** — збір, інтерпретація та застосування даних **К3** — спілкування з фахівцями, у т. ч. іноземною мовою	**Відповідальність та автономія** **АВ1** — управління складною технічною/професійною діяльністю **АВ2** — несення відповідальності за рішення в непередбачуваних контекстах **АВ3** — формування суджень із урахуванням соціальних, наукових та етичних аспектів **АВ4** — організація і керівництво професійним розвитком інших **АВ5** — здатність продовжувати навчання з високим ступенем автономії
ЗК1	**Зн2**	**Ум1**		
ЗК2	**Зн2**	**Ум1**	**К1**	
ЗК3			**К1, К3**	
ЗК4			**К1, К3**	
ЗК5	**Зн1, Зн2**	**Ум1**	**К2**	**АВ3**
ЗК6	**Зн1**		**К1**	**АВ2, АВ3, АВ4**
ЗК7			**К1**	**АВ2**
ЗК8	**Зн2**		**К2**	**АВ3**
СК1	**Зн2**	**Ум1**	**К2**	
СК2	**Зн1, Зн2**	**Ум1**	**К2**	
СК3		**Ум1**		**АВ1**
СК4		**Ум1**		**АВ1**
СК5		**Ум1**	**К2**	**АВ1, АВ2**
СК6		**Ум1**	**К1**	**АВ1**
СК7		**Ум1**	**К1**	**АВ1**
СК8	**Зн2**	**Ум1**		
СК9	**Зн2**	**Ум1**		
СК10		**Ум1**	**К2**	**АВ2**

Додаток Б

Таблиця 1. Матриця забезпечення програмних результатів навчання обов’язковими освітніми компонентами

	ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
РН01				+																											
РН02					+																										
РН03	+	+	+											+							+						+				
РН04														+	+	+		+		+		+	+	+	+	+			+	+	+
РН05											+				+									+			+	+		+	+
РН06								+	+	+								+	+										+	+	+
РН07											+		+								+								+	+	+
РН08						+	+				+				+			+												+	+
РН09														+							+	+					+	+	+	+	+
РН10								+	+		+												+	+		+		+	+	+	+
РН11																		+	+												
РН12										+							+									+					
РН13																	+									+		+			
РН14																			+		+		+	+							
РН15																			+								+				
РН16																												+			
РН17															+				+												
РН18													+									+									
РН19																						+									
РН20												+				+															
РН21																			+				+				+				
РН22																				+	+				+		+				
РН23																							+	+	+						
РН24																									+						
РН25														+							+				+		+				

Таблиця 2. Матриця відповідності компетентностей обов’язковим освітнім компонентам

	ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
ІК										+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 1				+	+									+		+			+	+		+	+	+	+	+	+	+	+	+
ЗК 2								+	+	+		+						+		+	+								+	+	+
ЗК 3				+																											
ЗК 4					+																										
ЗК 5		+				+	+				+		+																+		+
ЗК 6	+	+	+																												
ЗК 7	+	+	+											+							+										
ЗК 8	+	+	+			+	+																								
СК 1														+							+	+					+	+	+	+	+
СК 2								+	+		+												+	+		+		+	+	+	+
СК 3																		+	+												
СК 4										+							+									+					
СК 5																			+		+		+	+			+				
СК 6																												+			
СК 7															+				+												
СК 8													+									+									
СК 9												+				+															
СК 10																			+				+			+					
СК 11																				+	+		+	+			+				
СК 12																					+		+	+	+						

ЛИСТОК РЕЄСТРАЦІЇ ЗМІН

Номер зміни	Введення в дію	Що змінилося	Коли вступають в дію