

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

ЗАТВЕРДЖЕНО



Вчена рада Хмельницького
національного університету
протокол від 15 05 2025 р. № 14

Голова Вченої ради


Підпис

Микола СКИБА
Ім'я, ПРІЗВИЩЕ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Кібербезпека та захист інформації

РІВЕНЬ ВИЩОЇ ОСВІТИ

Перший (бакалаврський)

ГАЛУЗЬ ЗНАНЬ

F - Інформаційні технології

СПЕЦІАЛЬНІСТЬ

**F5 – Кібербезпека та захист
інформації**

ОСВІТНЯ КВАЛІФІКАЦІЯ

**Бакалавр з кібербезпеки та захисту
інформації**

Освітня програма вводиться у дію
з 01 09 2025 р.

Наказ від 23.06 2025р. № 57

Ректор


Підпис

Сергій МАТЮХ
Ім'я, ПРІЗВИЩЕ

ВНЕСЕНО

Кафедра кібербезпеки

Протокол від 14 03 2025 р. № 11

Зав. кафедри Юрій КЛЮЦ
Підпис Ім'я, прізвище

РОБОЧА ГРУПА

Гарант (Керівник робочої групи)

Віктор ЧЕШУН, канд. техн. наук, доц.
Підпис Ім'я, прізвище, науковий ступінь, вчений звання
cheshunvn@khmnu.edu.ua
E-mail гаранта

Члени робочої групи:

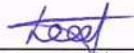
Олег САВЕНКО, д-р техн. наук, проф.
Підпис Ім'я, прізвище, науковий ступінь, вчений звання
Юрій КЛЮЦ, канд. техн. наук, доц.
Підпис Ім'я, прізвище, науковий ступінь, вчений звання
Віра ПІТОВА, канд. техн. наук, доц.
Підпис Ім'я, прізвище, науковий ступінь, вчений звання
Володимир АНІКІН
Підпис Ім'я, прізвище, науковий ступінь, вчений звання

ПОГОДЖЕНО:

Вчена рада факультету інформаційних технологій Протокол від <u>14</u> <u>03</u> 2025 р. № <u>8</u> Голова вченої ради <u>Тетяна ГОВОРУЩЕНКО</u> Підпис Ім'я, ПРІЗВИЩЕ	Навчально-методичний відділ Завідувач <u>Ірина АНДРОЩУК</u> Підпис Ім'я, ПРІЗВИЩЕ Відділ ліцензування, акредитації, моніторингу освітнього процесу та видачі документів про вищу освіту Завідувач <u>Ігор АНДРОЩУК</u> Підпис Ім'я, ПРІЗВИЩЕ Відділ забезпечення якості вищої освіти Завідувач <u>Ганна КРАСИЛЬНИКОВА</u> Підпис Ім'я, ПРІЗВИЩЕ
--	--

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
Кібербезпека та захист інформації

Голова студентської ради факультету інформаційних технологій
Назва


Підпис

Олеся БОСА
Ім'я, ПРІЗВИЩЕ

Заступник генерального директора з технічних питань
ТОВ ХмельницькІнфоком
Назва підприємства (організації, установи)



Вячеслав ВОВК
Ім'я, ПРІЗВИЩЕ

Начальник Управління цифрового розвитку, цифрових трансформацій та
цифровізації Хмельницької обласної військової адміністрації
Назва підприємства (організації, установи)



Олексій ФЕДОРОВ
Ім'я, ПРІЗВИЩЕ

Начальник Управління протидії кіберзлочинам у Хмельницькій області
Департаменту кіберполіції Національної поліції України
Назва підприємства (організації, установи)



Олег ДЯДИК
Ім'я, ПРІЗВИЩЕ

І Опис освітньої програми
Кібербезпека та захист інформації

(Назва освітньої програми)

зі спеціальності **F5 Кібербезпека та захист інформації**

Код і найменування спеціальності

1 Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Хмельницький національний університет Факультет інформаційних технологій Кафедра кібербезпеки
Рівень вищої освіти	Перший (бакалаврський)
Ступінь вищої освіти	Бакалавр
Форми здобуття освіти	Очна (денна)
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Професійна кваліфікація	Не присвоюється
Кваліфікація в дипломі	Ступінь вищої освіти – бакалавр Спеціальність – F5 - Кібербезпека та захист інформації Освітня програма – Кібербезпека та захист інформації
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації»
Тип диплома та обсяг освітньої програми	Диплом бакалавра – одиничний, обсяг освітньої програми – 240 кредитів ЄКТС, термін навчання – 3 роки і 10 місяців
Наявність акредитації	Первинна акредитація планується у 2028-2029 навчальному році
Цикл/рівень рамки кваліфікацій	НРК – 6 рівень; FQ-EHEA – перший цикл; EQF LLL – 6 рівень
Гарант освітньої програми (контактна інформація)	Чешун Віктор Миколайович, кандидат технічних наук, доцент cheshunvn@khnmu.edu.ua
Вимоги до освіти осіб, які можуть розпочати навчання за цією програмою	Наявність повної загальної середньої освіти
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступного оновлення ОП, відповідно до Положення про освітні програми підготовки здобувачів вищої освіти у ХНУ
Інтернет адреса постійного розміщення освітньої програми	Вебсайт Університету (https://khnmu.edu.ua/op/): розділ «Нормативні документи», рубрика «Освітні програми»

2 Мета освітньої програми	
Підготовка конкурентоздатних фахівців, які володіють загальними та фаховими компетентностями, здатні використовувати і впроваджувати технології та розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації, пов'язані із реалізацією комплексного підходу у впровадженні і підтримці архітектури систем кібербезпеки, а також з впровадженням, тестуванням, підтримкою та адмініструванням інформаційно-комунікаційних систем, обладнання та програмного забезпечення кіберзахисту.	
3 Характеристика освітньої програми	
Опис предметної області	Галузь знань: F Інформаційні технології Спеціальність: 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'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).
Орієнтація освітньої програми	Освітньо-професійна програма.
Особливості освітньої програми	Спеціальна освіта в галузі інформаційних технологій за спеціальністю «Кібербезпека та захист інформації». Акцент програми зроблено на поглибленій підготовці з встановлення та підтримки мереж і систем та їх компонентів й з адміністрування систем управління даними, що дозволяють безпечно зберігати, обробляти, запитувати, захищати та використовувати дані.
4 Можливості працевлаштування та подальшого навчання випускників	
Можливості працевлаштування	За Національним класифікатором професій (ДК 003:2010): 2139.2 Адміністратор безпеки мереж і систем 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 3439 Фахівець із організації інформаційної безпеки
Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.

5 Викладання та оцінювання	
Викладання та навчання	Лекції. Лабораторні, практичні та семінарські заняття. Практики. Самостійна робота. Словесні, наочні, практичні, частково-пошукові, проблемні, інтерактивні, проєктні методи навчання, технології ситуативного, позиційного та контекстного навчання, інформаційно-комунікаційні технології.
Оцінювання	Оцінювання навчальних досягнень здобувачів вищої освіти здійснюється за 100-бальною накопичувальною шкалою, яка трансформується в інституційну шкалу та шкалу ЄКТС. Захисти курсових проєктів, практик, лабораторних робіт; оцінювання результатів практичних і семінарських занять; усне опитування; тестування; іспити, заліки, диференційовані заліки; єдиний державний кваліфікаційний іспит тощо.
6 Програмні компетентності	
Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК)	ЗК01. Здатність застосовувати знання у практичних ситуаціях ЗК02. Знання та розуміння предметної області і розуміння професійної діяльності ЗК03. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК04. Здатність спілкуватися іноземною мовою. ЗК05. Здатність вчитися і оволодівати сучасними знаннями. ЗК06. 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 в Україні. ЗК07. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК08. 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.
Фахові (спеціальні, предметні) компетентності (ФК)	ФК01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. ФК02. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. ФК03. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. ФК04. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. ФК05. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

	ФК06. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) ФК07. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. ФК08. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. ФК09. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. ФК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
Унікальні компетентності, визначені освітньою програмою (УК)	УК01. Здатність налаштовувати та оптимізовувати мережеве обладнання, тестувати та підтримувати мережеву інфраструктуру включно із програмним та апаратним забезпеченням, діагностувати проблеми підключення до мережі та несправне апаратне забезпечення системи/сервера. УК02. Здатність впроваджувати стандарти управління даними та вимоги і специфікації, моніторити і підтримувати бази даних з метою забезпечення їх оптимальної продуктивності, виконувати резервне копіювання та відновлення баз даних для забезпечення цілісності даних, підтримувати програмне та інше забезпечення систем управління базами даних. УК03. Здатність ідентифікувати себе як громадянина України, здійснювати психологічну саморегуляцію та заходи щодо забезпечення безпеки й надання домедичної допомоги.
7 Програмні результати навчання (ПРН)	
ПРН01. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. ПРН02. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. ПРН03. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. ПРН04. 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. ПРН05. 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. ПРН06. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. ПРН07. 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. ПРН08. 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. ПРН09. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.	

ПРН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. ПРН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. ПРН13. 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. ПРН14. 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. ПРН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. ПРН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. ПРН17. 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 кількісної і якісної оцінки ризиків. ПРН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. ПРН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. ПРН20. 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. ПРН21. 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.	
Програмні результати навчання, визначені освітньою програмою (ПРН) ПРН22. Проводити планування, управління та обслуговування систем/серверів, встановлювати, налаштовувати, експлуатувати мережеве обладнання (маршрутизатори, комутатори, фایрволи, сервери, засоби передачі та відповідне апаратне обладнання), налаштовувати маршрути в мережах організації та розмежовувати доступи до ресурсів. ПРН23. Використовувати інструменти управління мережею для аналізу структур мережевого трафіку, діагностувати несправні системні компоненти. ПРН24. Підтримувати бази даних (резервування, відновлення, видалення даних, файли логу транзакцій тощо), проводити моніторинг показників продуктивності та доступності, створювати запити та звіти відповідного спрямування, оптимізувати продуктивність бази даних. ПРН25. Уміти характеризувати українську національну ідентичність та її ознаки: використовувати способи та методи психологічної саморегуляції й допомоги, способи забезпечення безпеки/самобезпеки в умовах надзвичайних ситуацій, надавати домедичну допомогу.	
8 Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення реалізації освітньої програми відповідає Ліцензійним умовам провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015 № 1187 (в редакції постанови КМУ від 24.03.2021 № 365).

Матеріально-технічне забезпечення	Матеріально-технічне забезпечення підготовки здобувачів вищої освіти відповідає Ліцензійним умовам провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015 № 1187 (в редакції постанови КМУ від 24.03.2021 № 365).
Інформаційне та навчально-методичне забезпечення	Інформаційне забезпечення становить: – наявність вітчизняних фахових періодичних видань відповідного спеціальності профілю; – доступ до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю; – офіційний веб-сайт університету, на якому розміщена основна інформація про ліцензії та сертифікати про акредитацію освітньої програми, діяльність, зразки документів про освіту, умови для доступності осіб з інвалідністю та інших маломобільних груп населення до приміщень, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація; – інформаційна система «Електронний університет»; – модульне середовище для навчання; – електронна бібліотека університету. Навчально-методичне забезпечення становить: – затверджена в установленому порядку освітньо-професійна програма, навчальні плани, за якими здійснюється підготовка здобувачів вищої освіти; – робочі програми з усіх навчальних дисциплін, що містять: програму навчальної дисципліни, заплановані результати навчання, порядок оцінювання результатів навчання, рекомендовану літературу (основну, додаткову), інформаційні ресурси в Інтернеті; – наскрізна програма практик; – методичні рекомендації до практик; – методичні рекомендації до виконання практичних і лабораторних робіт та семінарських занять; – методичні рекомендації до виконання курсових проєктів – програма єдиного державного кваліфікаційного іспиту
9 Академічна мобільність	
Національна кредитна мобільність	Згідно з укладеними договорами із вітчизняними закладами вищої освіти та науковими установами
Міжнародна кредитна мобільність	Згідно з укладеними договорами із закордонними закладами вищої освіти та науковими установами
Навчання іноземних здобувачів вищої освіти	Не передбачається

II Перелік компонентів освітньої програми та їх логічна послідовність

2.1 Перелік компонентів освітньої програми

Шифр КОП	Компоненти освітньої програми (КОП) (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційний іспит)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
Загальна підготовка (ОЗП)				
ОЗП.01	Вища математика	10	іспит	1,2
ОЗП.02	Дискретна математика	4	іспит	1
ОЗП.03	Алгоритмізація та програмування	14	залік	1,2
ОЗП.04	Фізичне виховання та основи здоров'я	3	залік	1
ОЗП.05	Англійська мова за професійним спрямуванням	6	залік	1,2
ОЗП.06	Теорія ймовірності та математична статистика	4	іспит	2
ОЗП.07	Фізика	6	іспит	2
ОЗП.08.1	Базова загальновійськова підготовка (теоретична підготовка)	3	диф.залік	3
ОЗП.08.2	Основи патріотичної, психологічної підготовки та першої домедичної допомоги		залік	
ОЗП.09	Громадянське суспільство, економіка та управління	4	залік	4
ОЗП.10	Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека	4	залік	5
ОЗП.11	Філософія	4	залік	7
ОЗП.12	Культурологія, етика, естетика, культура мовлення та доброчесність	5	залік	8
	Разом:	67		
Фахова підготовка (ОФП)				
ОФП.01	Основи інформаційної безпеки	13	залік	1,2
ОФП.02	Математичні основи захисту інформації	8	залік іспит	3 4
ОФП.03	Теорія інформації та кодування	5	іспит	3
ОФП.04	Сигнали і процеси в системах захисту інформації	5	іспит	3
ОФП.05	Захист інформації в інформаційно-комунікаційних системах	13	іспит	3, 4,5
ОФП.06	Захист інформації в інформаційно-комунікаційних системах (курсний проєкт)	2	диф.залік	4
ОФП.07	Стеганографія і стеганоаналіз	5	іспит	4
ОФП.08	Нормативно-правове забезпечення кібербезпеки	6	іспит	5
ОФП.09	Прикладна криптологія	9	іспит	5,6
ОФП.10	Адміністрування та захист баз і сховищ даних	4	залік	6

ОФП.11	Адміністрування та захист баз і сховищ даних (курсний проєкт)	2	диф.залік	6
ОФП.12	Комплексні системи захисту інформації	16	залік іспит	6,7,8
ОФП.13	Технології виявлення вразливостей та вторгнень	6	іспит	7
ОФП.14	Управління інформаційною безпекою	9	залік іспит	7,8
ОФП.15	Виробнича практика 1	5	диф.залік	6
ОФП.16	Виробнича практика 2	5	диф.залік	8
	Єдиний державний кваліфікаційний іспит		іспит	8
	Разом:	113		
Загальний обсяг обов'язкових компонентів		180		
ВИБІРКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
	Вибіркові освітні компоненти 3 семестру	10	залік*	3
	Вибіркові освітні компоненти 4 семестру	10	залік*	4
	Вибіркові освітні компоненти 5 семестру	10	залік*	5
	Вибіркові освітні компоненти 6 семестру	10	залік*	6
	Вибіркові освітні компоненти 7 семестру	10	залік*	7
	Вибіркові освітні компоненти 8 семестру	10	залік*	8
Загальний обсяг вибірових компонентів		60		
Загальний обсяг Освітньої програми		240		

Примітка:* Загальна кількість заліків залежить від числа вибраних здобувачами вищої освіти освітніх компонентів у семестрі

2.2 Логічна послідовність вивчення компонентів освітньої програми

Таблиця структурно-логічних зв'язків компонентів освітньої програми

Шифр КОП	Компоненти освітньої програми (КОП) (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційний іспит)	Семестр	Пререквізити	Постреквізити
ОЗП.01	Вища математика	1,2	Вихідна	ОЗП.06 ОЗП.07 ОФП.02 ОФП.04
ОЗП.02	Дискретна математика	1	Вихідна	ОФП.02 ОФП.03
ОЗП.03	Алгоритмізація та програмування	1,2	Вихідна	ОФП.10 ОФП.11 ОФП.13
ОЗП.04	Фізичне виховання та основи здоров'я	1	Вихідна	ОЗП.08.01 ОЗП.08.02 ОЗП.10
ОЗП.05	Англійська мова за професійним спрямуванням	1,2	Вихідна	ОЗП.12 ОФП.06 ОФП.08 ОФП.11 ОФП.14

ОФП.01	Основи інформаційної безпеки	1,2	Вихідна	ОФП.02 ОФП.05 ОФП.06 ОФП.08
ОЗП.06	Теорія ймовірності та математична статистика	2	ОЗП.01	ОФП.03 ОФП.04
ОЗП.07	Фізика	2	ОЗП.01	ОФП.04 ОЗП.10
ОЗП.08.01	Базова загальна військова підготовка	3	ОЗП.04	ОЗП.09 ОЗП.10
ОЗП.08.02	Основи патріотичної, психологічної підготовки та першої домедичної допомоги			
ОФП.03	Теорія інформації та кодування	3	ОЗП.02 ОЗП.06	ОФП.05 ОФП.06 ОФП.07 ОФП.09
ОФП.04	Сигнали і процеси в системах захисту інформації	3	ОЗП.01 ОЗП.06 ОЗП.07	ОЗП.10 ОФП.05 ОФП.06 ОФП.12
ОФП.02	Математичні основи захисту інформації	3,4	ОЗП.01 ОЗП.02 ОФП.01	ОФП.07 ОФП.09
ОФП.05	Захист інформації в інформаційно-комунікаційних системах	3,4,5	ОФП.01 ОФП.03 ОФП.04	ОФП.06 ОФП.12 ОФП.13 ОФП.15 ОФП.16
ОФП.06	Захист інформації в інформаційно-комунікаційних системах (курсний проєкт)	4	ОЗП.05 ОФП.01 ОФП.03 ОФП.04 ОФП.05	ОФП.12 ОФП.13 ОФП.15 ОФП.16
ОФП.07	Стеганографія і стеганоаналіз	4	ОФП.02 ОФП.03	ОФП.09 ОФП.15
ОЗП.09	Громадянське суспільство, економіка та управління	4	ОЗП.08.01 ОЗП.08.02	ОЗП.10 ОЗП.11 ОЗП.12 ОФП.14 ОФП.15 ОФП.16
ОЗП.10	Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека	5	ОЗП.04 ОЗП.07 ОЗП.08.01 ОЗП.08.02 ОФП.04 ОЗП.09	ОФП.15 ОФП.16
ОФП.08	Нормативно-правове забезпечення кібербезпеки	5	ОЗП.05 ОФП.01	ОФП.10 ОФП.11 ОФП.12 ОФП.13 ОФП.14 ОФП.15 ОФП.16
ОФП.09	Прикладна криптологія	4,5	ОФП.02 ОФП.03 ОФП.07	ОФП.12 ОФП.15 ОФП.16

ОФП.10	Адміністрування та захист баз і сховищ даних	6	ОЗП.03 ОФП.08	ОФП.11 ОФП.12 ОФП.13 ОФП.15 ОФП.16
ОФП.11	Адміністрування та захист баз і сховищ даних (курсний проєкт)	6	ОЗП.03 ОЗП.05 ОФП.08 ОФП.10	ОФП.12 ОФП.13 ОФП.15 ОФП.16
ОФП.15	Виробнича практика 1	6	ОЗП.09 ОЗП.10 ОФП.05 ОФП.06 ОФП.07 ОФП.08 ОФП.09 ОФП.10 ОФП.11	ОФП.13 ОФП.14 ОФП.16
ОФП.12	Комплексні системи захисту інформації	6,7,8	ОФП.04 ОФП.05 ОФП.06 ОФП.08 ОФП.09 ОФП.10 ОФП.11	ОФП.16
ОЗП.11	Філософія	7	ОЗП.09	ОЗП.12 ОФП.14 ОФП.16
ОФП.13	Технології виявлення вразливостей та вторгнень	7	ОЗП.03 ОФП.05 ОФП.06 ОФП.08 ОФП.10 ОФП.11 ОФП.15	ОФП.16
ОФП.14	Управління інформаційною безпекою	7,8	ОЗП.09 ОЗП.05 ОФП.08 ОФП.15 ОЗП.11	ОФП.16
ОЗП.12	Культурологія, етика, естетика, культура мовлення та доброчесність	8	ОЗП.05 ОЗП.09 ОЗП.11	ОФП.16
ОФП.16	Виробнича практика 2	8	ОЗП.09 ОЗП.10 ОЗП.11 ОЗП.12 ОФП.05 ОФП.06 ОФП.08 ОФП.09 ОФП.10 ОФП.11 ОФП.12 ОФП.13 ОФП.14 ОФП.15	

III Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до атестаційного іспиту/екзамену (за наявності)	Визначаються Порядком атестації здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту, затвердженим постановою Кабінету Міністрів України від 19 травня 2021 р. № 497.

IV Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Система внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) в університеті відповідає вимогам Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG), статті 16 чинного Закону України «Про вищу освіту» (зі змінами). Система внутрішнього забезпечення якості функціонує в Університеті на п'яти організаційних рівнях відповідно до Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти у Хмельницькому національному університеті (вебсайт Університету (<https://khmnu.edu.ua/>): розділ «Нормативні документи», рубрика – «Положення», сторінка – «Положення про організацію освітньої діяльності»).

Система внутрішнього забезпечення якості 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 університету та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті університету, на інформаційних стендах та 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 дотримання академічної доброчесності працівниками університету та здобувачами вищої освіти, у тому числі створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату;
- 9) інших процедур і заходів.

V Матриця відповідності програмних компетентностей компонентам освітньої програми

Матриця відповідності програмних компетентностей компонентам освітньої програми представлена в Додатку А.

VI Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

Матриця відповідності програмних результатів навчання компонентам освітньої програми представлена в Додатку Б.

VII Процедура присвоєння професійної кваліфікації

Не присвоюється.

Використані джерела

- 1 Закон України “Про освіту” (зі змінами) [Електронний ресурс]. – URL: <http://zakon3.rada.gov.ua/laws/show/2145-19>.
- 2 Закон “Про вищу освіту” (у редакції від 16.08.2024 р.) [Електронний ресурс]. – URL: <http://zakon4.rada.gov.ua/laws/show/1556-18>.
- 3 Постанова Кабінету Міністрів України «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» від 30.08.2024 р. № 1021 [Електронний ресурс]. – URL: <https://zakon.rada.gov.ua/laws/show/1021-2024-п#Text>.
- 4 «Про затвердження Порядку проведення базової загальної середньої підготовки громадян України, які здобувають вищу освіту, та поліцейських». Постанова Кабінету Міністрів України від 21 червня 2024 р. № 734. [Електронний ресурс]. – URL: <https://zakon.rada.gov.ua/laws/show/734-2024-п#Text>.
- 5 Національна рамка кваліфікацій (в редакції постанови Кабінету Міністрів України від 25 червня 2020 р. № 519). [Електронний ресурс]. – URL: <https://zakon.rada.gov.ua/laws/show/519-2020-п#Text>.
- 6 Національний класифікатор України: Класифікатор професій ДК 003:2010 (із змінами і доповненнями, внесеними наказом Міністерства економіки України від 16.01.2024 № 1410)
- 7 Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015 № 1187 (в редакції постанови КМУ від 24.03.2021 № 365).
- 8 «Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту». Постанова Кабінету Міністрів України від 19 травня 2021 № 497. [Електронний ресурс]. – URL: <https://zakon.rada.gov.ua/laws/show/497-2021-п#Text>.
- 9 Наказ МОН України «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затверджених постановою Кабінету Міністрів України від 30 серпня 2024 року № 1021» від 19.11.2024 р. № 1625 [Електронний ресурс]. – URL: <https://zakon.rada.gov.ua/laws/show/z1833-24#Text>.
- 10 Лист МОНУ від 05.06.2018 № 1/9-377 «Щодо надання роз’яснень стосовно освітніх програм».
- 11 Стандарт вищої освіти України зі спеціальності 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології», затверджений наказом МОНУ від 29 жовтня 2024 № 1547.
- 12 Професійний стандарт «Фахівець з підтримки інфраструктури кіберзахисту», затверджений Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України 23 січня 2024 року № 38.
- 13 Професійний стандарт «Адміністратор мереж і систем», затверджений Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України 25 листопада 2022 року № 715.
- 14 Лист МОНУ від 28.04.2017 № 1/9-239 «Зразок освітньо-професійної програми для першого та другого рівнів вищої освіти».
- 15 Методичні рекомендації до розроблення освітніх програм підготовки фахівців різних рівнів вищої освіти у ХНУ. [Електронний ресурс]. – URL: <https://msn.khmnpu.edu.ua/course/view.php?id=5838>.

V Матриця відповідності програмних компетентностей компонентам освітньої програми

[illegible]

