ПРОЄКТ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО

Вчена рада Хмельницького
національного університету
протокол від __ ___ 2025 р. №__

Голова Вченої ради
_____ Микола СКИБА
Підпис 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**

ЗАТВЕРДЖЕНО

Вченою радою ХНУ (Перша редакція)
протокол від _____ № _____

Освітня програма
вводиться у дію
з 01 09 2025 р.

Наказ від _____ 2025р. № ___

Ректор_____ Сергій МАТЮХ
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ВНЕСЕНО

Кафедра кібербезпеки

Протокол від ___ ____ 2025 р. № ____

Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, прізвище

РОБОЧА ГРУПА

Гарант (Керівник робочої групи)

_____ Віктор ЧЕШУН, канд. техн. наук, доц.
Підпис Ім'я, прізвище, вчений ступінь, звання

cheshunvn@khmnu.edu.ua
E-mail гаранта

Члени робочої групи:

_____ Олег САВЕНКО, д-р техн. наук, проф.
Підпис Ім'я, прізвище, вчений ступінь, звання

_____ Юрій КЛЬОЦ, канд. техн. наук, доц.
Підпис Ім'я, прізвище, вчений ступінь, звання

_____ Віра ТІТОВА, канд. техн. наук, доц.
Підпис Ім'я, прізвище, вчений ступінь, звання

_____ Володимир АНІКІН
Підпис Ім'я, прізвище, вчений ступінь, звання

ПОГОДЖЕНО:

Вчена рада факультету інформаційних технологій Протокол від ___ _____ 2025 р. № ____ Голова вченої ради _____ Тетяна ГОВОРУЩЕНКО Підпис Ім'я, ПРІЗВИЩЕ	**Навчально-методичний відділ** Завідувач _____ Лариса ЛЮБОХИНЕЦЬ а Підпис Ім'я, ПРІЗВИЩЕ **Відділ ліцензування, акредитації, моніторингу освітнього процесу та видачі документів про вищу освіту** Завідувач _____ Ігор АНДРОЩУК а Підпис Ім'я, ПРІЗВИЩЕ **Відділ забезпечення якості вищої освіти** Завідувач _____ Ганна КРАСИЛЬНИКОВА Підпис Ім'я, ПРІЗВИЩЕ

ЛИСТ ПОГОДЖЕННЯ

Представник________

Назва підприємства (організації, установи)

_____ _____

Підпис Ім’я, ПРІЗВИЩЕ

Представник _____

Назва підприємства (організації, установи)

_____ _____

Підпис Ім’я, ПРІЗВИЩЕ

(Підпис представника завіряє відділ кадрів підприємства (організації, установи))

Голова студентської ради факультету _____

Назва

_____ _____

Підпис Ім’я, ПРІЗВИЩЕ

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	Бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації»
Тип диплома та обсяг освітньої програми	Тип диплома – одиничний, обсяг освітньої програми – 240 кредитів ЄКТС, термін навчання – 3 роки і 10 місяців
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти, Україна 2021 рік. Сертифікат про акредитацію освітньої програми № 1927. Дата видачі 30.06.2021. Термін дії до 01.07.2026.
Цикл/рівень рамки кваліфікацій	Національна рамка кваліфікацій – 6 рівень; FQ-EHEA – перший цикл; EQF LLL – 6 рівень
Гарант освітньої програми (контактна інформація)	Чешун Віктор Миколайович cheshunvn@khmnu.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, відповідно до Положення про освітні програми підготовки здобувачів вищої освіти у ХНУ
Інтернет адреса постійного розміщення освітньої програми	https://khmnu.edu.ua/op/

2 Мета освітньої програми	
Підготовка конкурентоздатних фахівців, які володіють загальнокультурними та професійними компетентностями у галузі кібербезпеки та захисту інформації, здатних використовувати і впроваджувати технології та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації, пов'язані із реалізацією комплексного підходу в реалізації і підтримці архітектури систем кібербезпеки, а також з тестуванням, впровадженням, 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 кіберпросгору, 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 підготовки бакалавра.
Особливості освітньої програми	Спеціальна освіта в галузі інформаційних технологій за спеціальністю “Кібербезпека та захист інформації”. Акцент програми зроблено на встановлення та підтримку мереж і систем, їх конкретних компонентів та на адміністрування системи управління даними, що дозволяють безпечно зберігати, обробляти, запитувати, захищати та використовувати дані. Ключові слова: кібербезпека, безпека інформаційно-комунікаційних систем, комп’ютерні мережі, загрози і ризики, моніторинг, адміністрування, нормативно-правове забезпечення інформаційної безпеки, технічний захист інформації, криптографічний захист інформації, управління інформаційною безпекою.

4 Можливості працевлаштування та подальшого навчання випускників	
Можливості працевлаштування	Випускник освітнього рівня бакалавр після успішного виконання освітньої програми здатен виконувати професійну роботу і, відповідно до Національного класифікатора України: Класифікатор професій (ДК 003:2010), займати первинну посаду за категоріями: 2139.2 Адміністратор безпеки мереж і систем 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2132.2 Конструктор систем кібербезпеки
Подальше навчання	Здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
5 Викладання та оцінювання	
Викладання та навчання	Студентоцентроване, проблемно-орієнтоване навчання. Методи навчання словесні та наочні, практичні, проблемно-пошукові, індуктивні, дедуктивні, репродуктивні, навчання у співпраці, моделювання, застосування інформаційно-комп'ютерних технологій.
Оцінювання	**Оцінювання навчальних досягнень** здійснюється за інституційною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системою. **Форми контролю:** письмові екзамени, заліки, захисти курсових проєктів, звітів з лабораторних робіт та звітів з практик, виконання практичних завдань, тестування, 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)	ЗК1. Здатність застосовувати знання у практичних ситуаціях ЗК2. Знання та розуміння предметної області і 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 та свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення й 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.

Спеціальні (фахові, предметні) компетентності (ФК)	ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. ФК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. ФК3. Здатність забезпечувати неперервність бізпес-процесів згідно встановленої політики кібербезпеки та захисту інформації. ФК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. ФК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. ФК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) ФК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібеобезпекою. ФК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності. ФК9. 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 (за наявності) (УК)	УК1. 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. УК2. 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.

7 Програмні результати навчання (ПРН)

ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.
ПРН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
ПРН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
ПРН4. 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.
ПРН5. 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.

ПРН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
ПРН7. 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.
ПРН8. 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.
ПРН9. 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 (за наявності) (ПРН)

ПРН22. Проводити планування, управління та обслуговування систем/серверів, встановлювати, налаштовувати, експлуатувати мережеве обладнання (маршрутизатори, комутатори, файрволи, 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.

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 та закордонних фахових періодичних видань відповідного або спорідненого 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; – 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 вказівки до виконання практичних робіт.
9 Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Хмельницьким національним університетом та закладами вищої освіти України.
Міжнародна кредитна мобільність	Перспективи участі та стажування у науково-дослідних проєктах та програмах академічної мобільності за кордоном.
Навчання іноземних здобувачів вищої освіти	Не здійснюється

ІІ Перелік компонентів освітньої програми та їх логічна послідовність

2.1 Перелік компонентів освітньої програми

Код КОП	Компоненти освітньої програми (КОП) (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	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	Культурологія, етика, естетика, культура мовлення та доброчесність	4	залік	4
ОЗП.09	Громадянське суспільство, економіка та управління	4	залік	5
ОЗП.10	Філософія	4	залік	7
ОЗП.11	Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека	4	залік	8
	Разом:	63		
Фахова підготовка (ОФП)				
ОФП.01	Основи інформаційної безпеки	13	залік	1,2
ОФП.02	Математичні основи захисту інформації	10	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	16	іспит, курсовий проєкт	3,4, 5
ОФП.06	Стеганографія і стеганоаналіз	5	іспит	4
ОФП.07	Нормативно-правове забезпечення кібербезпеки	6	іспит	5
ОФП.08	Прикладна криптологія	9	іспит	5,6
ОФП.09	Адміністрування та захист баз і сховищ даних	6	іспит, курсовий проєкт	6
ОФП.10	Комплексні системи захисту інформації	16	залік, іспит	6,7, 8
ОФП.11	Технології виявлення вразливостей та вторгнень	6	іспит	7

ОФП.12	Управління інформаційною безпекою	9	залік, іспит	7,8
ОФП.13	Проєктно-технологічна практика	5	залік	6
ОФП.14	Професійна практика	6	залік	8
	Єдиний державний кваліфікаційний іспит		іспит	8
	Разом:	116		
Загальний обсяг обов'язкових компонентів		**180**		
ВИБІРКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
	Вибіркові дисципліни 3 семестру*	10	залік**	3
	Вибіркові дисципліни 4 семестру*	10	залік**	4
	Вибіркові дисципліни 5 семестру*	10	залік**	5
	Вибіркові дисципліни 6 семестру*	10	залік**	6
	Вибіркові дисципліни 7 семестру*	10	залік**	7
	Вибіркові дисципліни 8 семестру*	10	залік**	8
Загальний обсяг вибіркових компонентів		**60**		
Загальний обсяг Освітньої програми		**240**		

2.2 Логічна послідовність вивчення компонентів освітньої програми

Таблиця структурно-логічних зв'язків компонентів освітньої програми

Код КОП	**Компоненти освітньої програми (КОП) (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)**	**Семестр***	**Пререквізити**	**Кореквізити**
ОЗП.01	Вища математика	1, 2	Вихідна	Фізика Математичні основи захисту інформації Теорія ймовірності та математична статистика Сигнали і процеси в системах захисту інформації
ОЗП.02	Дискретна математика	1	Вихідна	Математичні основи захисту інформації Теорія інформації та кодування
ОЗП.03	Алгоритмізація та програмування	1, 2	Вихідна	Адміністрування та захист баз і сховищ даних Технології виявлення вразливостей та вторгнень
ОЗП.04	Фізичне виховання та основи здоров'я	1	Вихідна	Громадянське суспільство, економіка та управління Культурологія, етика, естетика, культура мовлення та доброчесність

ОЗП.05	Англійська мова за професійним спрямуванням	1, 2	Вихідна	Культурологія, етика, естетика, культура мовлення та доброчесність Нормативно-правове забезпечення кібербезпеки Управління інформаційною безпекою
ОФП.01	Основи інформаційної безпеки	1, 2	Вихідна	Математичні основи захисту інформації Нормативно-правове забезпечення кібербезпеки Захист інформації в інформаційно-комунікаційних системах
ОЗП.06	Теорія ймовірності та математична статистика	2	Вища математика	Теорія інформації та кодування Сигнали і процеси в системах захисту інформації
ОЗП.07	Фізика	2	Вища математика	Сигнали і процеси в системах захисту інформації
ОФП.03	Теорія інформації та кодування	3	Дискретна математика Теорія ймовірності та математична статистика	Прикладна криптологія Стеганографія і стеганоаналіз Захист інформації в інформаційно-комунікаційних системах
ОФП.04	Сигнали і процеси в системах захисту інформації	3	Вища математика Фізика Теорія ймовірності та математична статистика	Захист інформації в інформаційно-комунікаційних системах Комплексні системи захисту інформації
ОФП.02	Математичні основи захисту інформації	3, 4	Вища математика Дискретна математика Основи інформаційної безпеки	Стеганографія і стеганоаналіз Прикладна криптологія
ОФП.05	Захист інформації в інформаційно-комунікаційних системах	3, 4,5	Нормативно-правове забезпечення кібербезпеки Основи інформаційної безпеки Сигнали і процеси в системах захисту інформації	Технології виявлення вразливостей та вторгнень Комплексні системи захисту інформації Проєктно-технологічна практика
ОФП.06	Стеганографія і стеганоаналіз	4	Математичні основи захисту інформації Теорія інформації та кодування	Прикладна криптологія Проєктно-технологічна практика
ОФП.07	Нормативно-правове забезпечення кібербезпеки	5	Англійська мова за професійним спрямуванням Основи інформаційної безпеки	Комплексні системи захисту інформації Технології виявлення вразливостей та вторгнень Управління інформаційною безпекою Захист інформації в

				інформаційно-комуніка-ційних системах Адміністрування та захист баз і сховищ даних Проєктно-технологічна практика Професійна практика
ОЗП.08	Культурологія, етика, естетика, культура мовлення та доброчесність	4	Англійська мова за професійним спрямуванням Фізичне виховання та основи здоров'я	Громадянське суспільство, економіка та управління Філософія
ОФП.08	Прикладна криптологія	4, 5	Математичні основи захисту інформації Теорія інформації та кодування Стеганографія і стеганоаналіз	Комплексні системи захисту інформації Професійна практика
ОФП.09	Адміністрування та захист баз і сховищ даних	6	Нормативно-правове забезпечення кібербезпеки Алгоритмізація та програмування	Комплексні системи захисту інформації Технології виявлення вразливостей та вторгнень
ОЗП.09	Громадянське суспільство, економіка та управління	5	Культурологія, етика, естетика, культура мовлення та доброчесність Фізичне виховання та основи здоров'я	Філософія Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека
ОФП.13	Проєктно-технологічна практика	6	Захист інформації в інформаційно-комуніка-ційних системах Сигнали і процеси в системах захисту інформації Стеганографія і стеганоаналіз Адміністрування та захист баз і сховищ даних Нормативно-правове забезпечення кібербезпеки	Управління інформа-ційною безпекою Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека Професійна практика
ОФП.10	Комплексні системи захисту інформації	6, 7, 8	Нормативно-правове забезпечення кібербезпеки Сигнали і процеси в системах захисту інформації Прикладна криптологія Захист інформації в інформаційно-комуніка-ційних системах Адміністрування та захист баз і сховищ даних	Професійна практика
ОЗП.10	Філософія	7	Громадянське суспільство, економіка та управління Культурологія, етика, естетика, культура мовлення та доброчесність	Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека

ОФП.11	Технології виявлення вразливостей та вторгнень	7	Нормативно-правове забезпечення кібербезпеки Захист інформації в інформаційно-комуніка-ційних системах Алгоритмізація та програмування Адміністрування та захист баз і сховищ даних	Професійна практика
ОФП.12	Управління інформаційною безпекою	7, 8	Нормативно-правове забезпечення кібербезпеки Англійська мова за про-фесійним спрямуванням Проєктно-технологічна практика	Професійна практика
ОЗП.11	Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека	8	Громадянське суспільство, економіка та управління Філософія Проєктно-технологічна практика	Професійна практика
ОФП.14	Професійна практика	8	Нормативно-правове забезпечення кібербезпеки Прикладна криптологія Комплексні системи захисту інформації Управління інформа-ційною безпекою Технології виявлення вразливостей та вторгнень Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека Проєктно-технологічна практика	-

Примітка: * Перелік компонентів освітньої програми подається у логічній послідовності їх вивчення у семестрах.

ІІІ 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 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 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-%D0%BF#Text

4 Стандарт вищої освіти України зі спеціальності 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології», затверджений наказом МОНУ від 29 жовтня 2024 № 1547.

5 Методичні рекомендації щодо розроблення стандартів вищої освіти. Наказ МОНУ від 01.06.2016 № 600 (у редакції наказу МОНУ від 03.04.2024 № 441).

6 Лист МОНУ від 05.06.2018 № 1/9-377 «Щодо надання роз’яснень стосовно освітніх програм».

7 Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015 № 1187 (в редакції постанови КМУ від 24.03.2021 № 365).

8 Лист МОНУ від 28.04.2017 № 1/9-239 «Зразок освітньо-професійної програми для першого та другого рівнів вищої освіти».

9 Методичні рекомендації зі складання Концепції освітньої діяльності на заявленому рівні вищої освіти або за освітньою програмою ХНУ. [Електронний ресурс]. – URL: https://msn.khmnu.edu.ua/course/index.php?categoryid=98.

10 «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.

11 Національний класифікатор України: Класифікатор професій ДК 003:2010 (із змінами і доповненнями, внесеними наказом Міністерства економіки України від 16.01.2024 № 1410)

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 «Конструктор систем кібербезпеки», затверджений Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України 23 січня 2024 року № 38.

14 Професійний стандарт «Адміністратор мереж і систем», затверджений Наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України 25 листопада 2022 року № 715.

Додаток А

V Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОЗП.01	ОЗП.02	ОЗП.03	ОЗП.04	ОЗП.05	ОЗП.06	ОЗП.07	ОЗП.08	ОЗП.09	ОЗП.10	ОЗП.11	ОФП.01	ОФП.02	ОФП.03	ОФП.04	ОФП.05	ОФП.06	ОФП.07	ОФП.08	ОФП.09	ОФП.10	ОФП.11	ОФП.12	ОФП.13	ОФП.14
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК1						+						+	+	+	+	+	+	+	+		+	+	+	+	+
ЗК2												+				+	+	+	+		+	+	+	+	+
ЗК3								+																	
ЗК4					+																				
ЗК5	+	+	+			+	+						+	+											
ЗК6								+	+		+								+		+		+		
ЗК7								+	+																
ЗК8			+	+				+	+	+	+	+		+	+		+	+	+				+	+	+
ФК1																			+		+		+	+	+
ФК2			+									+				+	+	+		+	+	+	+	+	+
ФК3																							+		+
ФК4												+				+				+	+		+	+	+
ФК5												+				+				+		+	+		+
ФК6																					+				+
ФК7																							+		+
ФК8													+					+						+	+
ФК9																					+				+
ФК10																					+	+			+
УК1																+								+	+
УК2																				+				+	+

Додаток Б

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

	ОЗП.01	ОЗП.02	ОЗП.03	ОЗП.04	ОЗП.05	ОЗП.06	ОЗП.07	ОЗП.08	ОЗП.09	ОЗП.10	ОЗП.11	ОФП.01	ОФП.02	ОФП.03	ОФП.04	ОФП.05	ОФП.06	ОФП.07	ОФП.08	ОФП.09	ОФП.10	ОФП.11	ОФП.12	ОФП.13	ОФП.14
ПРН1								+																	
ПРН2					+																				
ПРН3								+	+																
ПРН4												+				+	+	+	+		+	+	+	+	+
ПРН5																			+		+	+	+	+	+
ПРН6			+	+				+	+	+	+	+							+				+	+	+
ПРН7						+						+	+	+	+		+	+	+						
ПРН8	+	+	+			+	+						+	+											
ПРН9											+								+		+		+	+	+
ПРН10			+									+				+	+	+		+	+	+	+	+	+
ПРН11																							+		+
ПРН12												+				+							+	+	
ПРН13																+				+	+			+	+
ПРН14												+				+				+			+		+
ПРН15																						+	+		
ПРН16																					+				+
ПРН17																							+		+
ПРН18													+					+						+	+
ПРН19																		+						+	+
ПРН20																					+				+
ПРН21																					+	+			+
ПРН22																+								+	+
ПРН23																+								+	+
ПРН24																				+				+	+