МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО

Вчена рада Хмельницького
національного університету
протокол від 30 квітня 2026 р. №17

Голова Вченої ради
_____ Микола СКИБА
Підпис Ім'я, ПРІЗВИЩЕ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека та аналіз кіберзагроз»

РІВЕНЬ ВИЩОЇ ОСВІТИ	**Другий (магістерський)**
ГАЛУЗЬ ЗНАНЬ	**F Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**F5 Кібербезпека та захист інформації**
ОСВІТНЯ КВАЛІФІКАЦІЯ	**Магістр з кібербезпеки та захисту інформації**

Освітня програма вводиться у дію
з 1 вересня 2026 р.

Наказ від 12 червня 2026 № 64

В.о ректора _____ Віктор ЛОПАТОВСЬКИЙ
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2026

ВНЕСЕНО

Кафедра кібербезпеки

Протокол від 17 02 2026 р. № 10

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

РОБОЧА ГРУПА

Гарант (Керівник робочої групи)

_____ Віра ТІТОВА, канд. техн. наук, доц.
Підпис Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання

titovav@khmnu.edu.ua
E-mail гаранта

Члени робочої групи:

_____ Олег САВЕНКО, д-р. техн. наук, проф.
Підпис Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання

_____ Юрій КЛЬОЦ, канд. техн. наук, доц.
Підпис Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання

_____ Віктор ЧЕШУН, канд. техн. наук, доц.
Підпис Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання

_____ Володимир АНІКІН
Підпис Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання

ПОГОДЖЕНО:

Вчена рада факультету інформаційних технологій

Протокол від 17 03 2026 р. № 11

Голова вченої ради _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Навчально-методичний відділ

Завідувач _____ Ірина АНДРОЩУК
Підпис Ім'я, ПРІЗВИЩЕ

Відділ ліцензування, акредитації, моніторингу освітнього процесу та видачі документів про вищу освіту

Завідувач _____ Ігор АНДРОЩУК
Підпис Ім'я, ПРІЗВИЩЕ

Відділ забезпечення якості вищої освіти

Завідувач _____ Наталія КАРВАЦКА
Підпис Ім'я, ПРІЗВИЩЕ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
Кібербезпека та аналіз кіберзагроз

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

Підпис Олексій ФЕДОРОВ
Ім'я, ПРІЗВИЩЕ

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

Підпис Вячеслав ВОВК
Ім'я, ПРІЗВИЩЕ

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

Підпис Олег ДЯДИК
Ім'я, ПРІЗВИЩЕ

Голова студентської ради факультету інформаційних технологій
Назва

Підпис Денис ГРОМСЬКИЙ
Ім'я, ПРІЗВИЩЕ

І. Опис освітньої програми

_____ Кібербезпека та аналіз кіберзагроз _____

(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	Другий (магістерський)
Ступінь вищої освіти	Магістр
Форми здобуття освіти	Очна (денна)
Освітня кваліфікація	Магістр з кібербезпеки та захисту інформації
Професійна кваліфікація	Не присвоюється
Кваліфікація в дипломі	Ступінь вищої освіти – магістр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – Кібербезпека та аналіз кіберзагроз
Офіційна назва освітньої програми	Освітньо-професійна програма Кібербезпека та аналіз кіберзагроз
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, обсяг освітньої програми – 90 кредитів ЄКТС, термін навчання – 1 рік 4 місяці
Наявність акредитації	Первинна акредитація планується у 2027-2028 навчальному році
Цикл/рівень рамки кваліфікацій	НРК – 7 рівень; FQ-EHEA – другий цикл; EQF LLL – 7 рівень
Гарант освітньої програми (контактна інформація)	Тітова Віра Юріївна, канд. техн. наук, доц. titovav@khmnu.edu.ua
Вимоги до освіти осіб, які можуть розпочати навчання за цією програмою	Наявність ступеня вищої освіти бакалавра
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	вебсайт Університету (https://khmnu.edu.ua/op/): розділ «Нормативні документи», рубрика «Освітні програми)
2. Мета освітньої програми	
Підготовка конкурентоздатних професіоналів у галузі кібербезпеки та захисту інформації, які володіють загальними та фаховими компетентностями, здатні здійснювати технічний аналіз, запобігання й нейтралізацію кіберзагроз, вразливостей та інцидентів у мережевих, хостових і прикладних інформаційних системах на основі сучасних міжнародних стандартів, методологій і практик кібербезпеки.	

3. Характеристика освітньої програми	
Опис предметної області	***F*** – Інформаційні технології; ***F5*** – Кібербезпека та захист інформації ***Об'єкти вивчення:*** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. ***Цілі навчання:*** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. ***Теоретичний зміст предметної області*** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. ***Методи, методики та технології*** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.

	Інструменти та обладнання. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна
Особливості програми	Особливістю програми є спрямованість на формування практичних умінь і навичок з технічного збирання, обробки та аналізу даних кібербезпеки, пов'язаних із виявленням кіберзагроз, вразливостей та інцидентів у мережевих, хостових і прикладних середовищах. Освітній процес передбачає опанування сучасних технологій виявлення та запобігання вторгненням, моніторингу мережевої та хостової безпеки, аналізу вразливостей і тестування на проникнення з використанням спеціалізованих інструментів і платформ. Акцент зроблено на оцінюванні стану кібербезпеки, а також на розробленні заходів реагування, технічного запобігання та нейтралізації реальних і потенційних загроз інформаційних систем.
4. Можливості працевлаштування та подальшого навчання випускників	
Можливості працевлаштування	Проєктна, виробнича, технологічна, управлінська, науково-дослідна, інноваційна, експертна та консультативна діяльність у сфері кібербезпеки та захисту інформації. Назви професій згідно з Національним класифікатором професій (ДК 003:2010): 2139.2 Аналітик з безпеки інформаційно-комунікаційних систем 2139.2 Аналітик загроз безпеки 2139.2 Аудитор інформаційних технологій (з кібербезпеки) 2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки) 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2139.2 Фахівець з реагування на інциденти кібербезпеки
Подальше навчання	Можливість продовжувати освіту на третьому (освітньо-науковому) рівні вищої освіти Набуття додаткових кваліфікацій в системі освіти дорослих
5. Викладання та оцінювання	
Викладання та навчання	Лекції. Практичні, семінарські, лабораторні заняття. Практика. Самостійна робота, консультації. Методи навчання пояснювально-ілюстративні, словесні, наочні, практичні, проблемного навчання, частково-пошукові, дослідницькі; технології навчання у співпраці, ситуативного моделювання, інформаційно-комп'ютерні технології.
Оцінювання	Оцінювання результатів здійснюється за 100-бальною накопичувальною шкалою, яка трансформується в інституційну шкалу та шкалу ЄКТС. Іспити, заліки, захисти лабораторних робіт, оцінювання практичних та семінарських занять, усне опитування, тестування, захист звіту з переддипломної практики, публічний захист кваліфікаційної роботи.
6. Програмні компетентності	
Інтегральна компетентність (ІК)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності (ЗК)	ЗК01. Здатність застосовувати знання у практичних ситуаціях. ЗК02. Здатність проводити дослідження на відповідному рівні. ЗК03. Здатність до абстрактного мислення, аналізу та синтезу. ЗК04. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК05. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові (спеціальні, предметні) компетентності (ФК)	ФК01. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. ФК02. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. ФК03. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК04. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. ФК05. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК06. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК07. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ФК08. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК09. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. ФК10. Здатність провадити науково-педагогічну діяльність,

	планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
Унікальні компетентності, визначені освітньою програмою (УК)	УК01. Здатність здійснювати багаторівневий аналіз подій кібербезпеки, виявляти аномалії, ознаки вторгнень і цільових (змішаних) кібератак, прогнозувати їх розвиток, а також формувати обґрунтовані рішення щодо реагування, запобігання та нейтралізації таких загроз. УК02. Здатність здійснювати моделювання та аналіз сценаріїв реалізації цільових (змішаних) кібератак, застосовувати методики тестування на проникнення з метою виявлення вразливостей інформаційних систем, оцінювання ефективності систем і засобів кіберзахисту та формування рекомендацій щодо їх вдосконалення.
7. Програмні результати навчання (ПРН)	
ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу	

ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проєкти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
Програмні результати навчання (ПРН), визначені за освітньою програмою
ПРН24. Здійснювати багаторівневий аналіз подій кібербезпеки на основі журналів подій, мережевого трафіку та даних систем моніторингу з метою виявлення аномалій, ознак вторгнень і цільових (змішаних) кібератак, прогнозування їх розвитку та оцінювання можливих наслідків. ПРН25. Здійснювати моделювання та аналіз сценаріїв реалізації цільових (змішаних) кібератак та застосовувати методики тестування на проникнення з метою виявлення вразливостей інформаційних систем, а також систем та засобів кіберзахисту. ПРН26. Оцінювати ефективність систем і засобів кіберзахисту, формувати аналітичні висновки та обґрунтовані рекомендації щодо реагування, технічного запобігання, нейтралізації подальших загроз і вдосконалення систем та засобів кіберзахисту за результатами аналізу подій кібербезпеки, моделювання сценаріїв кібератак і тестування на проникнення.
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 періодичних видань, які відповідають профілю кібербезпеки та захисту інформації; − доступ до баз даних періодичних наукових видань англійською мовою, які відповідають профілю кібербезпеки та захисту інформації; − 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 освітніх компонентів, 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; − програма переддипломної практики; − методичні рекомендації до виконання лабораторних робіт, проведення практичних і семінарських занять; − методичні рекомендації до виконання кваліфікаційної роботи.
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 здійснюється

ІІ. Перелік компонентів освітньої програми та їх логічна послідовність

2.1. Перелік компонентів освітньої програми

Шифр КОП	Компоненти освітньої програми (КОП) (навчальні дисципліни, практика, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підс. контролю	Семестр
Обов'язкові компоненти освітньої програми				
Загальна підготовка (ОЗП)				
ОЗП.01	Англійська мова за професійним спрямуванням	4	залік	1
ОЗП.02	Філософські проблеми наукового пізнання	4	іспит	1
ОЗП.03	Наукові методи, штучний інтелект та аналітика в кібербезпеці	4	залік	1
	Разом:	12		
Фахова підготовка (ОФП)				
ОФП.01	Інженерія та тестування безпеки інформаційних систем	10	іспит	1,2
ОФП.02	Операційний моніторинг та управління кібербезпекою	9	іспит	1,2
ОФП.03	Теорія криптографічних систем та інфраструктури ключів	5	іспит	2
ОФП.04	Переддипломна практика	16	диф. залік	3
ОФП.05	Кваліфікаційна робота	14	публічний захист	3
	Разом:	54		
	Загальний обсяг обов'язкових компонент:	66		
Вибіркові компоненти освітньої програми				
	Вибіркові освітні компоненти 1 семестру	8	залік*	1
	Вибіркові освітні компоненти 2 семестру	16	залік*	2
	Загальний обсяг вибіркових компонент:	24		
	Загальний обсяг освітньої програми:	90		

* Загальна кількість заліків буде залежати 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, практики, кваліфікаційна робота)	Семестр	Пререквізити	Постреквізити
ОЗП.01	Англійська мова за професійним спрямуванням	1	вихідна	ОФП.04, ОФП.05
ОЗП.02	Філософські проблеми наукового пізнання	1	вихідна	ОФП.04, ОФП.05
ОЗП.03	Наукові методи, штучний інтелект та аналітика в кібербезпеці	1	вихідна	ОФП.01 (2 семестр), ОФП.02 (2 семестр), ОФП.03, ОФП.04, ОФП.05
ОФП.01	Інженерія та тестування безпеки інформаційних систем	1,2	вихідна (1 семестр), ОЗП.03 (2 семестр)	ОФП.04, ОФП.05
ОФП.02	Операційний моніторинг та управління кібербезпекою	1,2	вихідна (1 семестр), ОЗП.03 (2 семестр)	ОФП.04, ОФП.05
ОФП.03	Теорія криптографічних систем та інфраструктури ключів	2	ОЗП.03	ОФП.04, ОФП.05
ОФП.04	Переддипломна практика	3	ОЗП.01, ОЗП.02, ОЗП.03, ОФП.01, ОФП.02, ОФП.03	ОФП.05
ОФП.05	Кваліфікаційна робота	3	ОЗП.01, ОЗП.02, ОЗП.03, ОФП.01, ОФП.02, ОФП.03, ОФП.04	-

III. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути оприлюднена в репозитарії Хмельницького національного університету. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

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

	ОЗП.01	ОЗП.02	ОЗП.03	ОФП.01	ОФП.02	ОФП.03	ОФП.04	ОФП.05
ІК	+	+	+	+	+	+	+	+
ЗК01			+	+	+	+	+	+
ЗК02			+			+	+	+
ЗК03		+	+	+	+	+	+	+
ЗК04				+	+	+	+	+
ЗК05	+	+	+	+	+	+	+	+
ФК01	+		+	+	+	+	+	+
ФК02	+		+	+	+	+	+	+
ФК03				+	+	+	+	+
ФК04				+	+		+	+
ФК05				+	+		+	+
ФК06				+	+		+	+
ФК07				+	+		+	+
ФК08				+		+	+	+
ФК09				+	+		+	+
ФК10				+	+	+	+	+
УК01			+		+		+	+
УК02				+	+		+	+

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

	ОЗП.01	ОЗП.02	ОЗП.03	ОФП.01	ОФП.02	ОФП.03	ОФП.04	ОФП.05
ПРН1	+	+	+	+	+	+	+	+
ПРН2			+	+	+	+	+	+
ПРН3			+			+	+	+
ПРН4			+	+	+	+	+	+
ПРН5		+	+				+	+
ПРН6				+	+	+	+	+
ПРН7			+	+	+	+	+	+
ПРН8				+	+	+	+	+
ПРН9				+	+		+	+
ПРН10				+	+		+	+
ПРН11				+	+		+	+
ПРН12				+	+		+	+
ПРН13				+		+	+	+
ПРН14				+	+		+	+
ПРН15	+	+	+	+	+	+	+	+
ПРН16				+	+	+	+	+
ПРН17		+	+				+	+
ПРН18				+	+	+	+	+
ПРН19			+	+	+	+	+	+
ПРН20	+		+	+	+	+	+	+
ПРН21			+	+	+	+	+	+
ПРН22			+			+	+	+
ПРН23	+		+	+	+	+	+	+
ПРН24			+		+		+	+
ПРН25				+	+		+	+
ПРН26				+	+		+	+

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» (зі змінами) [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-%D0%BF#Text

4 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

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-%D0%BF#Text

6 Стандарт вищої освіти України зі спеціальності 125 – Кібербезпека (другий (магістерський) рівень), затверджений наказом МОНУ від 18 березня 2021 №332

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

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

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

10 Методичні рекомендації зі складання освітніх програм підготовки здобувачів вищої освіти у ХНУ. [Електронний ресурс]. – URL: https://msn.khmnu.edu.ua/course/view.php?id=5838