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	**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 2025 р.

Наказ від _____ 2025 № ___

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)

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

titovav@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

_____ Віктор ЧЕШУН, 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 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 _____ Ганна КРАСИЛЬНИКОВА Підпис 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	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
Офіційна назва освітньої програми	Кібербезпека та захист інформації
Тип диплому та обсяг освітньої програми	Тип диплому – одиничний, обсяг освітньої програми – 90 кредитів ЄКТС, термін навчання – 1 рік 4 місяці
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти, Україна 2024 рік. Сертифікат про акредитацію освітньої програми № 7730. Дата видачі 08.05.2024. Термін дії до 01.07.2028.
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	https://khmnu.edu.ua/magistratura/
2. Мета освітньої програми	
Підготовка конкурентоздатних фахівців, які володіють загальнокультурними та професійними компетентностями у галузі кібербезпеки та захисту інформації, здатних розв’язувати задачі дослідницького та/або інноваційного характеру, пов’язані з аналізом, моніторингом, адмініструванням, підтримкою та оцінюванням безпеки інформаційних систем.	

3. Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	***F*** - Інформаційні технології; ***F5*** – Кібербезпека та захист інформації ***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, мережеве устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проєктування, 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 програма підготовки магістра. ***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.
Особливості програми	Спеціальна освіта в галузі інформаційних технологій за спеціальністю кібербезпека та захист інформації. Акцент програми зроблено на супроводження діяльності систем і мереж щодо захисту інформації підприємства/організації; аналіз заходів та ситуації з безпекою інформаційних систем.
4. Можливості працевлаштування та подальшого навчання випускників	
Можливості працевлаштування	Проєктна, виробнича, технологічна, управлінська, науково-дослідна, інноваційна, викладацька, 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-телекомунікаційних систем 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2139.2 Адміністратор безпеки мереж і систем
Подальше навчання	Можливість навчання за програмою третього (освітньо-наукового) рівня вищої освіти Набуття додаткових кваліфікацій в системі післядипломної освіти
5. Викладання та оцінювання	
Викладання та навчання	Студентоцентроване, проблемно-орієнтоване навчання. Методи навчання пояснювально-ілюстративні, словесні та наочні, практичні, частково-пошукові, дослідницькі, проблемно-пошукові, ігрові, навчання у співпраці. Навчання з застосуванням інформаційно-комп'ютерних технологій та технологій моделювання.
Оцінювання	Письмові іспити, заліки, захист лабораторних робіт, виконання практичних завдань, вирішення ситуаційних завдань, публічні виступи (дискусії), усне опитування, тестування, захист практики, кваліфікаційної роботи, тощо
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)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові, предметні) компетентності (ФК)	ФК1. 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. ФК2. 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. ФК3. Здатність досліджувати, розробляти і супроводжувати методи

	та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК4. 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. ФК5. 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. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК7. 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. ФК8. 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. ФК9. 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)	УК1. Здатність використовувати інструменти кіберзахисту для постійного моніторингу та аналізу системної активності, характеризувати та аналізувати мережевий трафік для виявлення аномальної активності (метадані), шкідливих дій, потенційних загроз мережевим ресурсам, слабких місць, методів експлуатації, впливу на систему та інформацію; забезпечувати своєчасне виявлення, ідентифікацію та попередження про можливі атаки/вторгнення, аномальні події та дії зі зловживання та відрізняти ці інциденти та події від штатної діяльності, проводячи дослідження, аналізування і кореляцію в широкому діапазоні всіх наборів вихідних даних; виконувати кореляцію подій, використовуючи інформацію, зібрану з різних джерел на підприємстві, щоб досягти усвідомлення ситуації та визначити ефективність спостережуваної атаки; надавати рекомендації до планів аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій. УК2. Здатність проводити тестування на проникнення розроблених

	додатків та/або систем, надавати вхідні дані для технологічних процесів системи управління ризиками; визначати програмне забезпечення та операційні системи мережевого пристрою на основі аналізу мережевого трафіку, визначати відображення мережі та дії операційної системи; надавати керівництву рекомендації щодо кібербезпеки на основі інформації про виявлені вразливості; розуміти мережеві топології для усвідомлення потоків даних через мережу, забезпечувати інтеграцію та впровадження міждоменних рішень у безпечному середовищі; впроваджувати заходи безпеки системи відповідно до встановлених процедур, визначених тактик атак та виявлених вразливостей для забезпечення конфіденційності, цілісності, доступності, аутентифікації та безвідмовності.

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, визначені за освітньою програмою
ПРН24. Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень, виконувати аналіз трафіку на рівні пакетів для виявлення аномальної активності (метадані), шкідливих дій, потенційних загроз мережевим ресурсам, слабких місць, методів експлуатації, впливу на систему та інформацію, збирати та аналізувати артефакти вторгнення, розпізнавати та класифікувати типи загроз і пов'язаних з ними атак, використовувати методику обробки інцидентів для усвідомлення ситуації та визначення ефективності спостережуваної атаки, визначати зв'язки та закономірності між подіями кібербезпеки, надавати рекомендації з кібербезпеки на основі виявлених загроз і атак.
ПРН25. Визначати, як має працювати система безпеки (включаючи її стійкість і надійність) і як зміни умов, операцій або середовища впливатимуть на ці результати, адаптувати методи та налаштовувати інструменти тестування на проникнення у відповідності до операційних процесів інформаційних систем та інформаційних активів, розробляти сценарії тестування на проникнення на основі методів та засобів забезпечення мережевої безпеки і джерел вразливостей інформаційних ресурсів, розпізнавати та класифікувати типи вразливостей і визначати вектори можливих атак, виявляти і демонструвати використання технічних вразливостей інформаційних систем в рамках чинного законодавства.

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; − програма професійної практики; − методичні вказівки до виконання лабораторних робіт/практичних/семінарських занять; − методичні рекомендації до виконання кваліфікаційної роботи
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 компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент освітньої програми

Код КОП	Компоненти освітньої програми (КОП) (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підс. контролю	Се-местр
Обов'язкові компоненти освітньої програми				
Дисципліни загальної підготовки (ОЗП)				
ОЗП.1	Англійська мова за професійним спрямуванням	4	залік	1
ОЗП.2	Філософські проблеми наукового пізнання	4	іспит	1
ОЗП.3	Методологія та організація наукових досліджень	4	залік	1
	Разом:	12		
Дисципліни професійної підготовки (ОФП)				
ОФП.1	Аналіз вразливостей, проєктування, адміністрування та підтримка кіберзахисту	9	іспит	1,2
ОФП.2	Моніторинг та менеджмент інформаційної безпеки	9	іспит	1,2
ОФП.3	Теорія криптосистем та управління криптографічними ключами	6	іспит	2
ОФП.4	Професійна практика	16	залік	3
ОФП.5	Кваліфікаційна робота	14	квал. робота	3
	Разом:	54		
	Загальний обсяг обов'язкових компонент:	66		
Вибіркові компоненти освітньої програми				
	Вибіркові дисципліни 1 семестру	8	залік*	1
	Вибіркові дисципліни 2 семестру	16	залік*	2
	Разом:	24		
	Загальний обсяг освітньої програми:	90		

* кількість заліків залежить від вибору студентами дисциплін вільного вибору

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.1	Англійська мова за професійним спрямуванням	1	-	ОФП.4
ОЗП.2	Філософські проблеми наукового пізнання	1	-	ОФП.4
ОЗП.3	Методологія та організація наукових досліджень	1	-	ОФП.4
ОФП.1	Аналіз вразливостей, проєктування, адміністрування та підтримка кіберзахисту	1	-	ОФП.1 (2 семестр) ОФП.2 (2 семестр)
ОФП.2	Моніторинг та менеджмент інформаційної безпеки	1	-	ОФП.1 (2 семестр) ОФП.2 (2 семестр)
ОФП.1	Аналіз вразливостей, проєктування, адміністрування та підтримка кіберзахисту	2	ОФП.1 (1 семестр) ОФП.2 (1 семестр)	ОФП.4
ОФП.2	Моніторинг та менеджмент інформаційної безпеки	2	ОФП.1 (1 семестр) ОФП.2 (1 семестр)	ОФП.4
ОФП.3	Теорія криптосистем та управління криптографічними ключами	2	-	ОФП.4
ОФП.4	Професійна практика	3	ОЗП.1 ОЗП.2 ОЗП.3 ОФП.1 ОФП.2 ОФП.3	ОФП.5
ОФП.5	Кваліфікаційна робота	3	ОФП.4	-

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 випускників освітньої програми «Кібербезпека та захист інформації» спеціальності F5 «Кібербезпека та захист інформації» 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 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 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 компетентностей компонентам освітньої програми

Компетент-ності	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10	УК1	УК2
ОЗП.1	+				+										+		
ОЗП.2	+		+		+										+		
ОЗП.3	+	+			+	+									+		
ОФП.1	+			+	+	+	+	+		+	+		+		+		+
ОФП.2	+			+	+	+	+	+	+	+		+		+	+	+	
ОФП.3	+			+	+	+	+	+					+		+		
ОФП.4	+	+	+	+	+	+	+	+							+		
ОФП.5	+	+	+	+	+	+	+	+							+		

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

Програмні результати навчання	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
ОЗП.1	+														+								+			
ОЗП.2	+				+										+		+									
ОЗП.3	+		+												+						+	+				
ОФП.1	+		+	+		+	+	+		+	+		+		+	+		+	+	+					+	+
ОФП.2	+			+		+	+	+	+	+		+		+	+	+		+	+		+			+		
ОФП.3	+		+	+			+	+					+		+	+		+	+	+						
ОФП.4	+	+					+								+	+	+	+	+	+			+			
ОФП.5	+	+		+	+		+								+	+	+		+	+	+		+			

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 (другий (магістерський) рівень), затверджений наказом МОНУ від 18 березня 2021 №332.

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 Професійний стандарт «Фахівець з підтримки інфраструктури кіберзахисту», затверджено адміністрацією Державної служби спеціального зв’язку та захисту інформації України, наказ №38 від 23.01.2024.

11 Професійний стандарт «Адміністратор мереж і систем», затверджено адміністрацією Державної служби спеціального зв’язку та захисту інформації України, наказ №715 від 25.11.2022.

12 Професійний стандарт «Аналітик з безпеки інформаційно-телекомунікаційних систем», затверджено адміністрацією Державної служби спеціального зв’язку та захисту інформації України, наказ №715 від 25.11.2022.