МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО

Вчена рада Хмельницького
національного університету
протокол від __ _____ 2021 р. №__

Голова Вченої ради

_____ _____
Підпис Ініціали, прізвище

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

РІВЕНЬ ВИЩОЇ ОСВІТИ	**другий (магістерський)**
СПЕЦІАЛЬНІСТЬ	**125 - «Кібербезпека»**
ГАЛУЗЬ ЗНАНЬ	**12 - «Інформаційні технології»**
ОСВІТНЯ КВАЛІФІКАЦІЯ	**магістр з кібербезпеки**

Освітня програма вводиться у дію
з 1 вересня 2021 р.

Наказ від ____ _____ 2021р. № ___

Ректор_____ _____
Підпис Ініціали, прізвище

Хмельницький 2021

ВНЕСЕНО

Кафедра кібербезпеки та комп'ютерних систем і мереж

Протокол від ____ _____ 2021 р. № ____

Зав. кафедри _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

ПРОЄКТНА ГРУПА

Гарант (Керівник проєктної групи)

_____ В.Ю. Тітова, к.т.н., доцент
Підпис Ініціали, прізвище, вчений ступінь, звання

Члени проєктної групи:

_____ О.С. Андрощук, д.т.н., професор
Підпис Ініціали, прізвище, вчений ступінь, звання

_____ Ю.П. Кльоц, к.т.н., доцент
Підпис Ініціали, прізвище, вчений ступінь, звання

_____ В.М. Чешун, к.т.н., доцент
Підпис Ініціали, прізвище, вчений ступінь, звання

_____ В.С. Орленко, к.т.н., доцент
Підпис Ініціали, прізвище, вчений ступінь, звання

ПОГОДЖЕНО:

Вчена рада факультету програмування та комп'ютерних і телекомунікаційних систем

Протокол від ____ _____2021р. № ____

Голова вченої ради _____ О.С. Савенко
Підпис Ініціали, прізвище

Навчально-методичний відділ

Завідувач _____ Л.С. Любохинець
Підпис Ініціали, прізвище

Навчальний відділ

Завідувач _____ О.Г. Самолюк
Підпис Ініціали, прізвище

Відділ забезпечення якості вищої освіти

Завідувач _____ Г.В. Красильникова
Підпис Ініціали, прізвище

І. Профіль освітньої програми зі спеціальності 125 «Кібербезпека»

1. Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Хмельницький національний університет Факультет програмування та комп'ютерних і телекомунікаційних систем Кафедра кібербезпеки та комп'ютерних систем і мереж
Ступінь вищої освіти	Магістр
Назва освітньої кваліфікації	Магістр з кібербезпеки
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека»
Тип диплому та обсяг освітньої програми	Тип диплому – одиничний, обсяг освітньої програми – 90 кредитів ЄКТС, термін навчання – 1,5 роки
Наявність акредитації	Первинна акредитація планується у 2022-23 році
Цикл/рівень	НРК – 7 рівень; FQ-EHEA – другий цикл; EQF LLL – 7 рівень
Передумови	Наявність ступеня вищої освіти бакалавра
Мова(и) викладання	Українська
Термін дії освітньої програми	5 років
Інтернет адреса постійного розміщення освітньої програми	https://www.khnu.km.ua/root/page.aspx?l=0&r=50&p=5&f=M
2. Мета освітньої програми	
Набуття теоретичних і практичних знань та вмінь, навичок та інших компетентностей для успішної професійної діяльності у галузі кібербезпеки, пов'язаної з розв'язуванням задач дослідницького та інноваційного характеру у сферах управління інформаційною безпекою об'єктів інформаційної діяльності та критичної інфраструктури і захисту конфіденційності, доступності та цілісності інформаційних активів від загроз та вразливостей.	
3. Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Спеціалізована ***12*** - Інформаційні технології; ***125*** - Кібербезпека
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.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі інформаційних технологій за спеціальністю кібербезпека. Акцент програми зроблено на набуття знань, умінь та компетенцій в галузі управління інформаційною безпекою та дослідження, розробки та супроводу систем інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. Ключові слова: аудит та моніторинг інформаційної безпеки інформаційних систем і технологій; програмні, програмно-апаратні, технічні та криптографічні засоби захисту інформації; системи управління інформаційною безпекою; системи управління доступом, управління ризиками, управління кіберінцидентами; аналіз захищеності систем, комплексів та засобів кіберзахисту.
Особливості програми	Інтеграція знань з перспективних напрямів кібербезпеки, зокрема, сучасних методів аналізу та синтезу сучасних систем інформаційної безпеки в галузі управління інформаційною безпекою.
4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Проєктна, виробнича, технологічна, управлінська, науково-дослідна; інноваційна, викладацька, експертна та консультативна діяльність у сфері кібербезпеки. Назви професій згідно з Державним класифікатором професій (ДК 003:2010): Професіонал з інформаційно-комунікаційних технологій Професіонал із організації захисту інформації з обмеженим доступом Професіонал із організації інформаційної безпеки
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, 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.
Оцінювання	Письмові екзамени, заліки, диференційовані заліки, презентації, захист лабораторних робіт, виконання практичних завдань, захисти практики, курсових проєктів, 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.

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 проекти 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.
8. Ресурсне забезпечення реалізації програми

Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують викладання на освітньо-професійній програмі, за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи. Всі викладачі мають рівень наукової та професійної активності, який засвідчується виконанням не менше чотирьох видів та результатів ліцензійних вимог. До організації навчального процесу залучаються професіонали з досвідом роботи за фахом.
Матеріально-технічне забезпечення	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.
Інформаційне та навчально-методичне забезпечення	Наявність електронних ресурсів та програмного забезпечення: електронна бібліотека, інституційний репозитарій, електронний журнал, доступ до баз даних періодичних наукових видань англійською мовою, модульне середовище для навчання MOODLE. Навчальний план та пояснювальна записка до нього, робочі програми з навчальних дисциплін, комплекси навчально-методичного забезпечення дисциплін, програми наскрізної практичної підготовки, методичні матеріали для проведення атестації здобувачів.

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 проектах 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

Шифр	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підс. контро-лю	Семестр
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 (ОПП)				
ОПП.1	Моніторинг та менеджмент інформаційної безпеки	5	іспит	1
ОПП.2	Теорія та проектування захищених систем	5	іспит	1
ОПП.3	Проектування та супровід систем інформаційної безпеки	5	іспит, КП	2
ОПП.4	Методи аналізу та побудови криптосистем	5	іспит	2
ОПП.5	Моделювання та оцінювання ефективності засобів захисту інформації	4	іспит	2
ОПП.6	Науково-професійна практика	15	диф. залік	3
ОПП.7	Кваліфікаційна робота	15	кваліф. 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		

2.2. Структурно-логічна схема освітньої програми.

Структурно-логічна схема підготовки визначає науково-методичне структурування процесу реалізації освітньої програми, тобто короткий опис логічної послідовності вивчення компонент освітньої програми. Схему представлено у вигляді графа (Додаток А).

ІІІ. Форми атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Кібербезпека» спеціальності 125 «Кібербезпека» здійснюється у формі публічного захисту кваліфікаційної роботи та завершується видачею диплома встановленого зразка про присудження особі ступеня магістра із присвоєнням кваліфікації магістр з кібербезпеки. Атестація здійснюється відкрито і публічно. Кваліфікаційна робота має бути перевірена на академічний плагіат та оприлюднена на офіційному сайті або в репозитарії університету.

IV. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Система внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти (далі – СВЗЯ) в Університеті відповідає вимогам Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG), статті 16 Закону України «Про вищу освіту» (2014) та статті 41 Закону України «Про освіту» (2017). Створена СВЗЯ функціонує на п'яти організаційних рівнях відповідно до розроблених нормативних документів, що розміщені на сайті Університету: http://www.khnu.km.ua/root/page.aspx?r=700&p=100.

Система внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти містить:

1) стратегію (політику) та процедури забезпечення якості освіти;
2) систему та механізми забезпечення академічної доброчесності;
3) оприлюднені критерії, правила і процедури оцінювання здобувачів освіти;
4) оприлюднені критерії, правила і процедури оцінювання педагогічної (науково-педагогічної) діяльності педагогічних та науково-педагогічних працівників;
5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, в тому числі для самостійної роботи здобувачів освіти;
6) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;
7) забезпечення наявності інформаційних систем для ефективного управління закладом освіти;
8) створення у закладі освіти інклюзивного освітнього середовища, універсального дизайну та розумного пристосування;
9) інші процедури та заходи, що визначаються спеціальними законами або документами.

V. Матриця відповідності програмних компетентностей компонентам освітньої програми

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

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

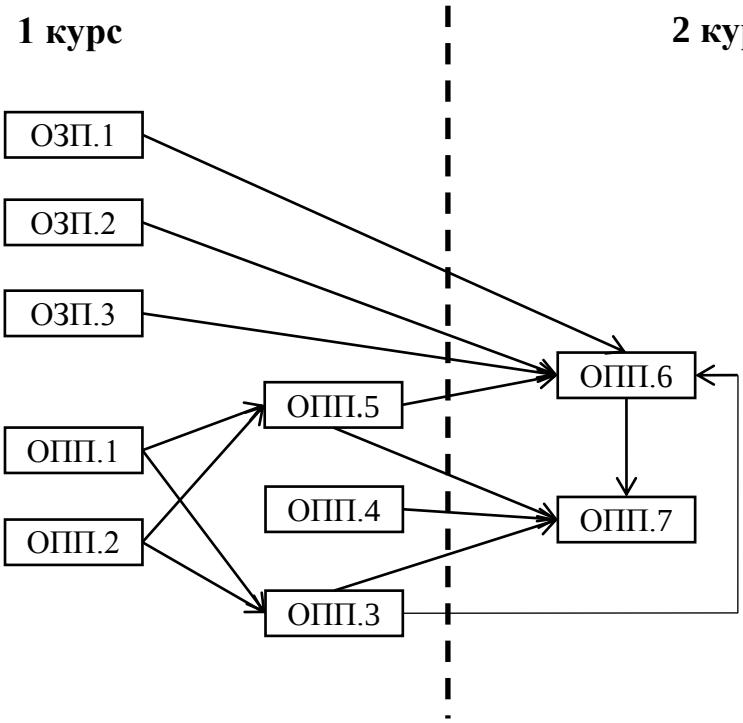
Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми представлена в Додатку В.

Використані джерела

1. Закон України "Про освіту" [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2145-19.
2. Закон "Про вищу освіту" [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18.
3. Рівні Національної рамки кваліфікацій [Електронний ресурс]. – Режим доступу: https://mon.gov.ua/ua/osvita/nacionalna-ramka-kvalifikacij/rivni-nacionalnoyi-ramki-kvalifikacij.
4. Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. Постанова КМУ від 29.04.2015 № 266 (зі змінами) [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/266-2015-%D0%BF.
5. Стандарт вищої освіти України зі спеціальності 125 – Кібербезпека (другий (магістерський) рівень), затверджений наказом МОНУ від 18 березня 2021 №332.
6. Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015 № 1187 (в редакції постанови КМУ від 10 травня 2018 р. № 347).
7. Методичні рекомендації до розроблення освітніх програм підготовки фахівців різних рівнів вищої освіти у Хмельницькому національному університеті (схвалені Науково-методичною радою університету, протокол від 26.12.2018 № 4).
8. Лист МОНУ від 05.06.2018 № 1/9-377 «Щодо надання роз'яснень стосовно освітніх програм».
9. Лист МОНУ від 28.04.2017 № 1/9-239 «Зразок освітньо-професійної програми для першого та другого рівнів вищої освіти».

Додаток А

Структурно-логічна схема освітньої програми



Додаток Б

Матриця відповідності програмних компетентностей компонентам освітньої програми

Компе-тентності	ОЗП.1	ОЗП.2	ОЗП.3	ОПП.1	ОПП.2	ОПП.3	ОПП.4	ОПП.5	ОПП.6	ОПП.7
ЗК1									+	+
ЗК2			+							
ЗК3		+							+	+
ЗК4								+		+
ЗК5	+								+	
ФК1								+		
ФК2									+	+
ФК3						+				
ФК4				+						
ФК5				+	+	+				
ФК6						+				
ФК7				+						
ФК8					+		+			
ФК9				+						
ФК10									+	

Додаток В

Матриця забезпечення результатів навчання відповідними компонентами освітньої програми

Програмні результати навчання	ОЗП.1	ОЗП.2	ОЗП.3	ОПП.1	ОПП.2	ОПП.3	ОПП.4	ОПП.5	ОПП.6	ОПП.7
ПРН1	+									
ПРН2									+	+
ПРН3			+		+		+			
ПРН4						+		+		
ПРН5		+							+	+
ПРН6							+	+		
ПРН7									+	+
ПРН8						+				
ПРН9				+						
ПРН10				+						
ПРН11						+				
ПРН12				+						
ПРН13					+		+			
ПРН14				+						
ПРН15									+	
ПРН16						+		+	+	+
ПРН17									+	
ПРН18									+	
ПРН19			+		+	+			+	+
ПРН20						+			+	+
ПРН21							+	+		+
ПРН22			+							+
ПРН23										+