

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

ЗАТВЕРДЖЕНО

Вчена рада Хмельницького
національного університету
протокол від ____ 2023 р. № ____

Голова Вченої ради

Підпис

М.Є. Скиба
Ініціали, прізвище

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека та захист інформації»

РІВЕНЬ ВИЩОЇ ОСВІТИ

другий (магістерський)

СПЕЦІАЛЬНІСТЬ

**125 - «Кібербезпека та захист
інформації»**

ГАЛУЗЬ ЗНАНЬ

12 - «Інформаційні технології»

ОСВІТНЯ КВАЛІФІКАЦІЯ

**магістр з кібербезпеки та захисту
інформації**

**Освітня програма вводиться у дію
з 1 вересня 2023 р.**

Наказ від ____ 2023р. № ____

Ректор _____

Підпис

С.А. Матюх
Ініціали, прізвище

Хмельницький 2023

ВНЕСЕНО

Кафедра кібербезпеки

Протокол від _____ 2023 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:

_____ А.В. Горошко, 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:

<p>Вчена рада факультету інформаційних технологій</p> <p>Протокол від _____ 2023 р. № _____</p> <p>Голова вченої ради _____ <u>О.С. Савенко</u> Підпис Ініціали, прізвище</p>	<p>Навчально-методичний відділ</p> <p>Завідувач _____ <u>Л.С. Любохинець</u> Підпис Ініціали, прізвище</p> <p>Навчальний відділ</p> <p>Завідувач _____ <u>О.Г. Самолук</u> Підпис Ініціали, прізвище</p> <p>Відділ забезпечення якості вищої освіти</p> <p>Завідувач _____ <u>Г.В. Красильникова</u> Підпис Ініціали, прізвище</p>
--	---

I. Профіль освітньої програми зі спеціальності 125 «Кібербезпека та захист інформації»

1. Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Хмельницький національний університет Факультет інформаційних технологій Кафедра кібербезпеки
Ступінь вищої освіти	Магістр
Назва освітньої кваліфікації	Магістр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Освітньо-професійна програма «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	Первинна акредитація планується у 2024-25 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	
2. Мета освітньої програми	
Набуття теоретичних і практичних знань та вмінь, навичок та інших компетентностей для успішної професійної діяльності у галузі кібербезпеки та захисту інформації, пов'язаної з аналітичною діяльністю, дослідженням, моніторингом та оцінюванням безпеки інформаційних систем.	
3. Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	<p>Спеціалізована 12 - Інформаційні технології; 125 – Кібербезпека та захист інформації</p> <p>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.</p> <p>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</p>

	<p>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.</p> <p>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.</p>
<p>Орієнтація освітньої програми</p>	<p>Освітньо-професійна програма підготовки магістра.</p> <p>Об'єкти вивчення:</p> <ul style="list-style-type: none"> – 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.
<p>Основний фокус освітньої програми та спеціалізації</p>	<p>Спеціальна освіта в галузі інформаційних технологій за спеціальністю кібербезпека та захист інформації. Акцент програми зроблено на збирання, оброблення, аналіз та поширення результатів оцінювання кіберзагроз; аналіз заходів та ситуації з безпекою інформаційних систем; дослідження, аналіз та участь у реагуванні на кіберінциденти в кіберпросторі.</p> <p>Ключові слова: моніторинг інформаційної безпеки інформаційних систем; реагування на кіберінциденти; програмні, програмно-апаратні, апаратні та криптографічні засоби захисту інформації; системи контролю доступом; управління ризиками; аналіз захищеності систем, комплексів та засобів кіберзахисту; тестування на проникнення та етичний хакінг.</p>
<p>Особливості програми</p>	<p>Інтеграція знань з перспективних напрямів кібербезпеки та захисту інформації, зокрема, сучасних методів аналізу безпеки інформаційних систем, аналізу загроз інформаційної безпеки, аналізу систем захисту інформації та оцінки вразливостей, реагування на інциденти кібербезпеки.</p>

4. Придатність випускників до працевлаштування та подальшого навчання

Придатність до працевлаштування	Проектна, виробнича, технологічна, управлінська, науково-дослідна; інноваційна, викладацька, експертна та консультативна діяльність у сфері кібербезпеки та захисту інформації. Назви професій згідно з Державним класифікатором професій (ДК 003:2010): 1226.2 Керівник структурного підрозділу (сфера захисту інформації) 1226.2 Начальник відділення (сфера захисту інформації) 2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем 2139.2 Аналітик загроз безпеки 2139.2 Аналітик систем захисту інформації та оцінки вразливостей 2139.2 Фахівець з реагування на інциденти кібербезпеки 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2 Фахівець з тестування систем захисту інформації 2139.2 Фахівець з підтримки інфраструктури кіберзахисту 2139.2 Фахівець сфери захисту інформації 2139.2 Фахівець з криптографічного захисту інформації 2139.2 Фахівець з технічного захисту інформації
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, 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 (КЗ)	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові,	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти

<p>предметні) компетентності (КФ)</p>	<p>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.</p> <p>КФ2. 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.</p> <p>КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</p> <p>КФ4. 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.</p> <p>КФ5. 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.</p> <p>КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.</p> <p>КФ7. 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.</p> <p>КФ8. 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.</p> <p>КФ9. 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.</p> <p>КФ10. 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.</p>
<p>7. Результати навчання (РН)</p>	
<p>РН1. 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</p>	

та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. 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.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. 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.

РН13. 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.

РН14. 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.

РН15. 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.

РН16. 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.

РН17. 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.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.

РН19. 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.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. 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.

РН23. 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 напрямку 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	Прикладне та спеціалізоване програмне забезпечення, маршрутизатори, керовані комутатори, міжмережеві екрани, апаратні шифратори, генератор віброакустичного зашумлення, пристрій захисту від ПЕМВ, генератори перешкод, система контролю доступу, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків).
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

II. 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. контролю	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	Етичний хакінг та тестування на проникнення	5	іспит	1
ОПП.2	Проектування та супровід систем захисту інформації	5	іспит	2
ОПП.3	Моніторинг та аудит інформаційної безпеки	9	іспит	1,2
ОПП.4	Криптосистеми та управління криптографічними ключами	5	іспит	2
ОПП.5	Професійна практика	15	диф. залік	3
ОПП.6	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).

III. Форми атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Кібербезпека та захист інформації» спеціальності 125 «Кібербезпека та захист інформації» здійснюється у формі публічного захисту кваліфікаційної роботи та завершується видачею диплома встановленого зразка про присудження особі ступеня магістра із присвоєнням кваліфікації магістр з кібербезпеки та захисту інформації. 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: <https://khmnu.edu.ua/normatyvni-dokumenty/>.

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 компетентностей компонентам освітньої програми

Матриця відповідності компетентностей компонентам освітньої програми представлена в Додатку Б.

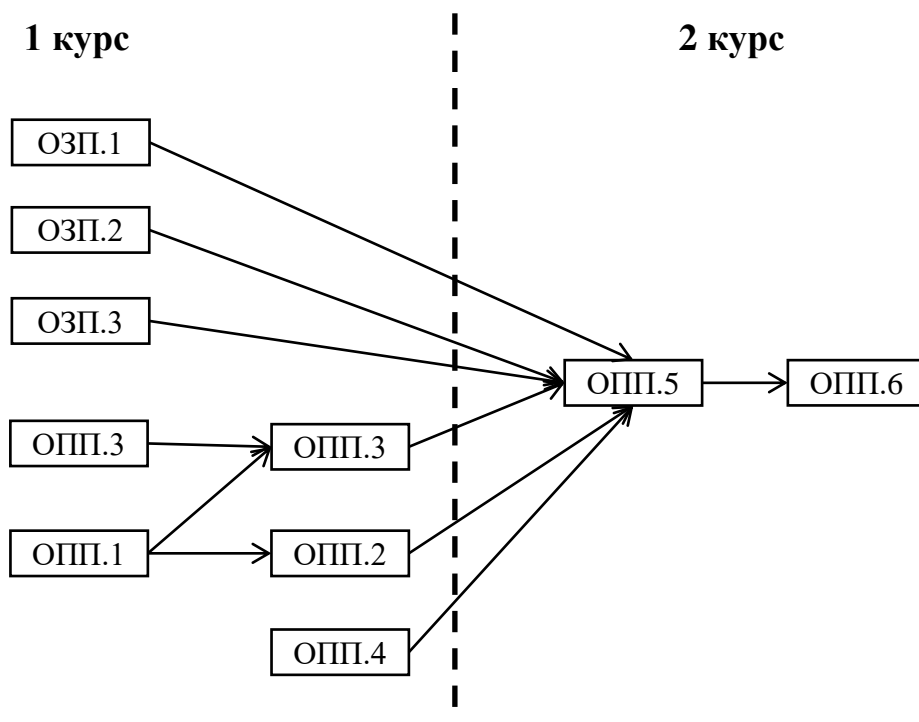
VI. Матриця забезпечення результатів навчання (РН) відповідними компонентами освітньої програми

Матриця забезпечення результатів навчання (РН) 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».

Структурно-логічна схема освітньої програми



Матриця відповідності компетентностей компонентам освітньої програми

Компетентності	ОЗП.1	ОЗП.2	ОЗП.3	ОПП.1	ОПП.2	ОПП.3	ОПП.4	ОПП.5	ОПП.6
КЗ1	+							+	+
КЗ2			+						
КЗ3		+							+
КЗ4						+			+
КЗ5	+	+	+					+	
КФ1			+	+	+		+	+	+
КФ2								+	+
КФ3					+		+		
КФ4						+			
КФ5				+		+			
КФ6					+				
КФ7						+			
КФ8					+		+		
КФ9						+			
КФ10		+		+		+		+	+

