МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО

Вчена рада Хмельницького
національного університету
протокол від 24 06 2021 р. № 18

Голова Вченої ради
_____ М.Є Скиба
Підпис Ініціали, прізвище

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека»

РІВЕНЬ ВИЩОЇ ОСВІТИ	**перший (бакалаврський)**
СПЕЦІАЛЬНІСТЬ	**125 - Кібербезпека**
ГАЛУЗЬ ЗНАНЬ	**12 - Інформаційні технології**
ОСВІТНЯ КВАЛІФІКАЦІЯ	**бакалавр з кібербезпеки**

Освітня програма вводиться у дію
з 1 вересня 2021 р.

Наказ від 29 06 2021р. № 81

Ректор _____ С.А. Матюх
Підпис Ініціали, прізвище

Хмельницький 2021

ВНЕСЕНО

Кафедра кібербезпеки та комп'ютерних систем і мереж

Протокол від 31 05 2021 р. № 11

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

ПРОЄКТНА ГРУПА

Гарант (Керівник проєктної групи)

_____ В.М. Чешун, 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.Ю. Тітова, 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 16 06 2021р. № 7

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

Профіль освітньої програми зі спеціальності
125 КІБЕРБЕЗПЕКА
Код і найменування спеціальності

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	Бакалавр
Офіційна назва освітньої програми	Освітньо-професійна програма «Кібербезпека»
Освітня кваліфікація	Бакалавр з кібербезпеки
Тип диплому та обсяг освітньої програми	Тип диплому – одиничний, обсяг освітньої програми – 240 кредитів ЄКТС, термін навчання – 4 роки
Наявність акредитації	Первинна акредитація, 2021 рік
Цикл/рівень	Національна рамка кваліфікацій – 6 рівень; FQ-EHEA – перший цикл; EQF LLL – 6 рівень
Передумови	Наявність повної загальної середньої освіти
Мова викладання	Українська
Термін дії освітньої програми	4 роки
Інтернет адреса постійного розміщення освітньої програми	https://www.khnu.km.ua/root/page.aspx?l=0&r=50&p=5&f=%D0%91
2. Мета освітньої програми	
Підготовка висококваліфікованих та конкурентоспроможних фахівців зі ступенем вищої освіти бакалавр, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, пов'язаних із забезпеченням цілісного підходу до захисту систем від атак хакерів, вірусів, несанкціонованого доступу до конфіденційних даних тощо у різних сферах професійної діяльності	
3. Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань - 12 Інформаційні технології Спеціальність - 125 Кібербезпека Об'єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.

	Теоретичний зміст предметної області Знання – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна програма. Здатність організовувати та підтримувати комплекс заходів інформаційної та/або кібербезпеки у різних сферах професійної діяльності відповідно до наявних ризиків та імовірних загроз згідно вимог національних та міжнародних стандартів і практик, законодавчої та нормативно-правової бази України.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі інформаційних технологій за спеціальністю кібербезпека. Акцент програми зроблено на розробці, впровадженні та супроводі комплексних систем захисту інформації, що базується на аналізі, виявленні та оцінюванні можливих загроз, уразливостей і дестабілізуючих чинників інформаційному простору та інформаційним ресурсам, та на ризик-орієнтованому контролі доступу до інформаційних ресурсів. Ключові слова: кібербезпека; інформаційна безпека, інформаційно-комунікаційні системи, загрози і ризики, моніторинг, програмні і програмно-апаратні засоби захисту, технічні засоби захисту, криптографічний захист, антивірусний захист, стандарти інформаційної безпеки, політики інформаційної та/або кібербезпеки, системи управління інформаційною та/або кібербезпекою.
Особливості програми	Інтегрована підготовка фахівців до вирішення завдань у сфері інформаційної та/або кібербезпеки, що передбачає розроблення, впровадження та експлуатацію комплексних (інформаційних, телекомунікаційних, технічних) систем і заходів захисту інформації на об’єктах інформаційної діяльності.

4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускник освітнього рівня бакалавр після успішного виконання освітньої програми здатен виконувати професійну роботу і, відповідно до Національного класифікатора України: Класифікатор професій (ДК 003:2010), займати первинну посаду за категоріями: 3439 Фахівець із організації інформаційної безпеки 3439 Фахівець із організації захисту інформації з обмеженим доступом
Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5. Викладання та оцінювання	
Викладання та навчання	Студентоцентроване, проблемно-орієнтоване навчання, яке реалізується у формах проблемних лекцій, практичних занять в малих групах, практикумів, лабораторних робіт, самостійної роботи, різних видів практик, виконання індивідуальних завдань, курсових проєктів та кваліфікаційної роботи тощо. Поєднуються класичні (пояснювально-ілюстративні, репродуктивні, практичні) та інноваційні (проблемні, проєктні, продуктивні, інтерактивні, ігрові, тренінгові, навчання у співпраці, модульно-розвивальні, розвитку критичного мислення, контекстні, моделювання, інформаційно-комп'ютерні тощо) технології навчання.
Оцінювання	Оцінювання навчальних досягнень здійснюється за інституційною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системою. Види контролю: вхідний, поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестування, вирішення ситуаційних завдань, публічні виступи, практична перевірка (ділові ігри, презентації), захисти звітів з лабораторних робіт, звітів з практик, курсових проєктів, кваліфікаційної роботи тощо.
6. Перелік компетентностей випускника	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації. ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності (ФК)	ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

	ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7. Програмні результати навчання (ПРН)	
ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки. ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки. ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.	

ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.
ПРН 12. Розробляти моделі загроз та порушника.
ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
ПРН 21. Вирішувати задачі забезпечення та супроводу (в т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.
ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.
ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки.
ПРН 36. Виявляти небезпечні сигнали технічних засобів.
ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.
ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

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 стаж педагогічної роботи. В ході організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи.
Матеріально-технічне забезпечення	Для організації навчального процесу за освітньою програмою використовуються спеціалізовані лабораторії, комп'ютерні класи, аудиторії для проведення практичних і лекційних занять: – спеціалізовані лабораторії випускової кафедри: лабораторія програмних і програмно-апаратних засобів захисту; лабораторія безпеки інформаційно-комунікаційних систем; лабораторія комплексних систем захисту. – лінгафонний кабінет з лінгафонним комплексом, аудіо і відео апаратурою для занять з іноземних мов. – комп'ютерні класи інформаційно-комп'ютерного центру університету з сучасною комп'ютерною технікою, мережевим обладнанням, програмним забезпеченням, вільним доступом до інформаційних ресурсів університету та мережі Internet. – аудиторії для проведення практичних і лекційних занять з використанням мультимедійних засобів; – лекційні зали з мультимедійним обладнанням. У всіх приміщеннях університету забезпечено вільний і необмежений доступ до Wi-Fi. Наявні приміщення, лабораторії, їх обладнання і програмне забезпечення дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.
Інформаційне та навчально-методичне забезпечення	Наявність забезпечення відповідно до ліцензійних умов: – періодичні видання, що відповідають профілю спеціальності, у науковій бібліотеці (у тому числі в електронному вигляді); – доступ до публікацій наукометричних баз Scopus, Web of Science; – офіційний веб-сайт ХНУ, на якому розміщена основна інформація про організацію навчального процесу; – модульне середовище для навчання MOODLE; – наукова бібліотека університету, електронна бібліотека університету; – освітня програма, навчальний план, робочі програми з усіх навчальних дисциплін навчального плану; – програми практичної підготовки; – методичні вказівки до виконання лабораторних робіт і практичних занять; – програма і методичні матеріали для проведення атестації здобувачів.
9. Академічна мобільність	
Національна кредитна мобільність	Реалізація на основі двосторонніх договорів між Хмельницьким національним університетом та закладами вищої освіти України: Херсонським національним технічним університетом, Луцьким національним технічним університетом, Київським національним університетом імені Тараса Шевченка, Чернівецьким національним університетом імені Юрія Федьковича, Запорізьким національним університетом, іншими навчальними закладами тощо.
Міжнародна кредитна мобільність	Реалізація на основі двосторонніх договорів між Хмельницьким національним університетом та закладами вищої освіти країн ЄС, проходження практик і стажування за кордоном та у представництвах іноземних фірм в Україні.
Навчання іноземних здобувачів вищої освіти	Не здійснюється

ІІ. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент освітньої програми

Шифр КОП	Компоненти освітньої програми (КОП) (навчальні дисципліни, курсові проекти, практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
Загальна підготовка (ОЗП)				
ОЗП.01	Вища математика	12	іспит	1,2
ОЗП.02	Дискретна математика	4	іспит	1
ОЗП.03	Технології програмування та алгоритмізації	8	іспит	1
ОЗП.04	Фізичне виховання та основи здоров'я	3	залік	1
ОЗП.05	Англійська мова за професійним спрямуванням	6	залік	1, 2
ОЗП.06	Теорія ймовірності та математична статистика	5	іспит	2
ОЗП.07	Фізика	6	іспит	2
ОЗП.08	Громадянське суспільство, економіка та управління	4	залік	5
ОЗП.09	Культурологія, культура мовлення, етика та естетика	4	залік	6
ОЗП.10	Філософія	4	залік	7
ОЗП.11	Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека	5	іспит	8
	Разом:	61		
Професійна підготовка (ОПП)				
ОПП.01	Основи інформаційної безпеки	6	залік	1
ОПП.02	Операційні системи та технології їх захисту	5	залік	2
ОПП.03	Теорія інформації та кодування	5	залік	2
ОПП.04	Сигнали і процеси в системах захисту інформації	6	іспит	3
ОПП.05	Прикладна криптологія	9	іспит, курсова робота	3
ОПП.06	Захист інформації в інформаційно-комунікаційних системах	9	іспит, курсовий проект	3,4
ОПП.07	Безпека вебресурсів	5	залік	4
ОПП.08	Компонентна база і схемотехніка систем захисту	6	іспит	4
ОПП.09	Технічний і криптографічний захист інформації	5	іспит, курсовий проект	4
ОПП.10	Нормативно-правове забезпечення кібербезпеки	5	іспит	5
ОПП.11	Безпека безпроводових технологій та інтернету речей	5	іспит	5
ОПП.12	Адміністрування та захист баз і сховищ даних	6	іспит, курсовий проект	5
ОПП.13	Системи контролю доступу	6	іспит	6
ОПП.14	Технології виявлення вразливостей та вторгнень	5	іспит	6

Шифр КОП	Компоненти освітньої програми (КОП) (навчальні дисципліни, курсові проекти, практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
ОПП.15	Моделювання систем захисту даних, оцінка ризиків і прийняття рішень	5	іспит	7
ОПП.16	Комплексні системи захисту інформації	6	іспит, курсовий проект	7
ОПП.17	Управління інформаційною безпекою	5	іспит	7
ОПП.18	Проєктно-технологічна практика	5	залік	6
ОПП.19	Переддипломна практика	5	залік	8
ОПП.20	Кваліфікаційна робота	10	кваліфікаційна робота	8
	Разом	119		
Загальний обсяг обов'язкових компонентів		180		
ВИБІРКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
	Вибіркові дисципліни 3 семестру*	10	залік**	3
	Вибіркові дисципліни 4 семестру*	10	залік**	4
	Вибіркові дисципліни 5 семестру*	10	залік**	5
	Вибіркові дисципліни 6 семестру*	10	залік**	6
	Вибіркові дисципліни 7 семестру*	10	залік**	7
	Вибіркові дисципліни 8 семестру*	10	залік**	8
Загальний обсяг вибіркових компонентів		**60**		
Загальний обсяг освітньої програми		**240**		

Примітки:

* Перелік вибіркових дисциплін визначається за результатами вільного вибору студентів;

** Кількість заліків залежить від вибору студентами дисциплін вільного вибору.

2.2. Структурно-логічна схема освітньої програми

Структурно-логічна схема підготовки визначає процес реалізації Освітньої програми, тобто короткий опис логічної послідовності вивчення компонент Освітньої програми. Структурно-логічну схему представлено у вигляді графа (Додаток А).

2.3. Вибіркові компоненти освітньої програми

Вибіркові компоненти освітньої програми здобувачі вищої освіти обирають з університетського каталогу вибіркових дисциплін, який формується з навчальних дисциплін, наданих різними кафедрами за різними рівнями вищої освіти. Кредитність вибіркових навчальних дисциплін кратна 4, передбачена можливість вибору односеместрових дисциплін та дисциплін, викладання яких розподіляється на 2 семестри (по 2 кредити). Щорічно перелік вибіркових освітніх компонент від кожної кафедри оновлюється. Здобувачі вищої освіти за даною ОПП повинні вибрати у кожному з 3-8 семестрів 2-3 дисципліни сумарною кількістю 10 кредитів ЄКТС. Процедура вибору здійснюється у терміни, встановлені Положенням про порядок реалізації права здобувачів вищої освіти на вільний вибір навчальних дисциплін у Хмельницькому національному університеті (https://www.khnu.km.ua/root/files/01/06/03/162.pdf). Каталог вибіркових дисциплін розміщено на сайті університету www.khnu.km.ua.

III. Форми атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності 125 «Кібербезпека» здійснюється у формі публічного захисту кваліфікаційної роботи та завершується видачею диплома встановленого зразка про присудження особі ступеня бакалавра із присвоєнням кваліфікації Бакалавр з кібербезпеки.

Кваліфікаційна робота не повинна містити академічного плагіату та фальсифікації.

Кваліфікаційні роботи оприлюднюються на офіційному сайті Інституційного репозитарію Хмельницького національного університету (http://elar.khnu.km.ua/jspui/).

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, що розміщене в рубриці «Публічна інформація» (Режим доступу : http://khnu.km.ua/root/files/01/06/03/024.pdf).

Система внутрішнього забезпечення якості передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду Освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників університету та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті університету, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною Освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про Освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення дотримання академічної доброчесності працівниками університету та здобувачами вищої освіти, у тому числі створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату;

9) інших процедур і заходів.

V. Матриця відповідності програмних компетентностей компонентам освітньої програми

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

VI. Матриця забезпечення результатів навчання відповідними компонентами освітньої програми

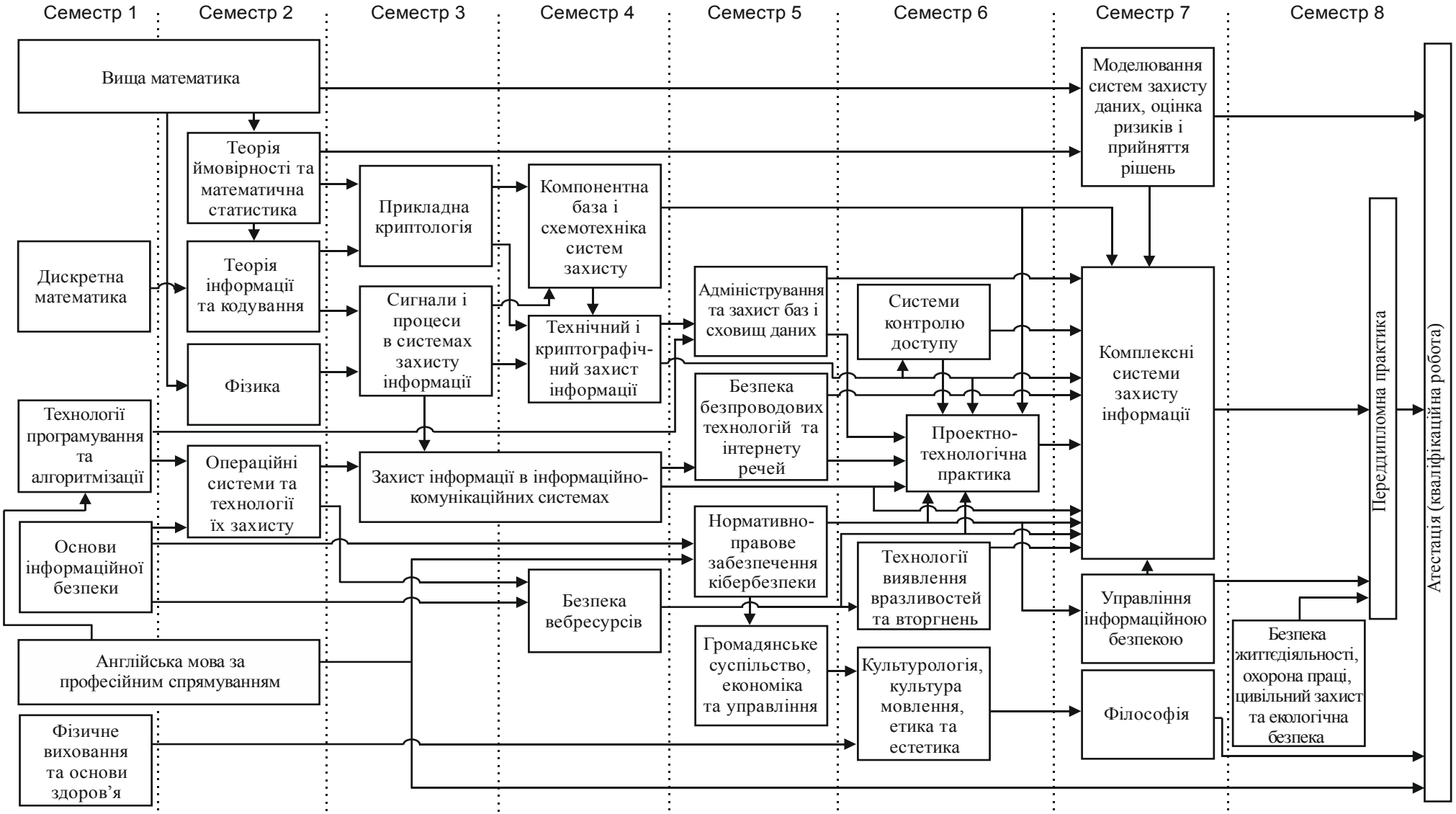
Матриця забезпечення результатів навчання відповідними компонентами освітньої програми представлена в Додатку В.

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. Стандарт вищої освіти України зі спеціальності 125 – Кібербезпека, затверджений наказом МОНУ від 04 жовтня 2018 № 1074.
5. Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015 № 1187 (в редакції постанови КМУ від 10 травня 2018 р. №347).
6. Методичні рекомендації щодо розроблення стандартів вищої освіти. Наказ МОНУ від 01.06.2017 № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584).
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

V. Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОЗП.01	ОЗП.02	ОЗП.03	ОЗП.04	ОЗП.05	ОЗП.06	ОЗП.07	ОЗП.08	ОЗП.09	ОЗП.10	ОЗП.11	ОПП.01	ОПП.02	ОПП.03	ОПП.04	ОПП.05	ОПП.06	ОПП.07	ОПП.08	ОПП.09	ОПП.10	ОПП.11	ОПП.12	ОПП.13	ОПП.14	ОПП.15	ОПП.16	ОПП.17	ОПП.18	ОПП.19	ОПП.20
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 1	+	+	+		+	+	+	+			+			+	+	+			+		+							+		+	+
ЗК 2									+	+				+							+									+	+
ЗК 3					+				+																					+	+
ЗК 4																									+	+		+		+	+
ЗК 5										+							+				+		+				+			+	+
ЗК 6				+				+	+	+	+	+									+									+	
ЗК 7				+					+	+	+																				
ФК 1																					+			+				+	+	+	+
ФК 2												+	+	+		+	+	+		+	+	+	+	+	+	+	+	+		+	+
ФК 3			+									+	+				+					+	+		+	+	+		+	+	
ФК 4																										+		+		+	+
ФК 5														+			+								+	+	+		+	+	+
ФК 6												+	+										+					+	+	+	
ФК 7																											+			+	+
ФК 8																					+				+			+		+	
ФК 9																								+		+	+	+		+	+
ФК 10																+			+						+					+	
ФК 11															+		+			+					+		+	+	+	+	
ФК 12																	+			+		+	+	+	+	+	+			+	+

Додаток В

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

	ОЗП.01	ОЗП.02	ОЗП.03	ОЗП.04	ОЗП.05	ОЗП.06	ОЗП.07	ОЗП.08	ОЗП.09	ОЗП.10	ОЗП.11	ОПП.01	ОПП.02	ОПП.03	ОПП.04	ОПП.05	ОПП.06	ОПП.07	ОПП.08	ОПП.09	ОПП.10	ОПП.11	ОПП.12	ОПП.13	ОПП.14	ОПП.15	ОПП.16	ОПП.17	ОПП.18	ОПП.19	ОПП.20
ПРН 1					+				+																				+	+
ПРН 2																									+		+		+	+
ПРН 3										+							+				+		+				+			+	+
ПРН 4																									+	+		+		+	+
ПРН 5	+	+	+		+	+	+	+			+			+	+	+			+		+							+		+	+
ПРН 6									+	+				+							+									+	+
ПРН 7																					+							+	+	+	+
ПРН 8																					+			+				+		+	
ПРН 9																									+			+		+	+
ПРН 10																	+													+	+
ПРН 11																							+								+
ПРН 12																									+						+
ПРН 13																	+					+									+
ПРН 14												+										+	+			+	+		+		
ПРН 15																	+					+			+				+	+	
ПРН 16																											+				+
ПРН 17																	+									+				+	
ПРН 18																									+		+		+	+	
ПРН 19														+		+	+			+										+	+
ПРН 20													+																+		
ПРН 21																								+			+			+	
ПРН 22													+				+													+	
ПРН 23													+				+	+		+		+	+		+					+	
ПРН 24																					+			+				+		+	+
ПРН 25																								+			+			+	
ПРН 26																	+									+				+	
ПРН 27														+			+								+		+				+

	ОЗП.01	ОЗП.02	ОЗП.03	ОЗП.04	ОЗП.05	ОЗП.06	ОЗП.07	ОЗП.08	ОЗП.09	ОЗП.10	ОЗП.11	ОПП.01	ОПП.02	ОПП.03	ОПП.04	ОПП.05	ОПП.06	ОПП.07	ОПП.08	ОПП.09	ОПП.10	ОПП.11	ОПП.12	ОПП.13	ОПП.14	ОПП.15	ОПП.16	ОПП.17	ОПП.18	ОПП.19	ОПП.20
ПРН 28																									+	+	+			+	+
ПРН 29																									+	+	+			+	+
ПРН 30																				+				+	+	+				+	
ПРН 31												+						+				+								+	+
ПРН 32												+	+										+					+	+	+	
ПРН 33								+																		+				+	+
ПРН 34																								+				+		+	+
ПРН 35																										+				+	
ПРН 36															+					+						+					
ПРН 37																				+						+					
ПРН 38															+					+						+					
ПРН 39																								+		+	+		+		
ПРН 40															+					+						+					
ПРН 41																	+								+		+				
ПРН 42																									+		+		+	+	
ПРН 43																					+				+		+		+		
ПРН 44																										+	+		+	+	
ПРН 45																										+	+				
ПРН 46																										+			+	+	
ПРН 47																+			+										+		
ПРН 48																+									+				+		
ПРН 49																	+												+		
ПРН 50																									+			+			
ПРН 51																	+								+			+			
ПРН 52																	+								+		+	+	+		
ПРН 53			+																												
ПРН 54				+				+	+	+	+										+								+		