ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО

Вчена рада Хмельницького національного університету
Протокол від 30.03 2017 №11
Голова Вченої ради
_____ М.Є. Скиба
30.08 2017 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Вид освітньої програми

«КІБЕРБЕЗПЕКА»

Назва освітньої програми

РІВЕНЬ ВИЩОЇ ОСВІТИ Перший (бакалаврський)

СПЕЦІАЛЬНІСТЬ 125 «Кібербезпека»
Код і найменування

ГАЛУЗЬ ЗНАНЬ 12 «Інформаційні технології»
Шифр і назва

ОСВІТНЯ КВАЛІФІКАЦІЯ Бакалавр з кібербезпеки
Назва

ВНЕСЕНО

Кафедра кібербезпеки та комп'ютерних систем і мереж

Протокол від 14 02 2017 № 7

В.о. зав. кафедри _____ В.М. Джулій
Підпис Ініціали, прізвище

Проектна група

Керівник проектної групи

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

Члени проектної групи:

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

_____ І. В. Муляр, к.т.н., доцент
Підпис Ініціали, прізвище, вчений ступінь, звання

_____ В.О. Бойчук, к.т.н., доцент
Підпис Ініціали, прізвище, вчений ступінь, звання

ПОГОДЖЕНО

Вчена рада факультету програмування та комп'ютерних і телекомунікаційних систем
Протокол від 17 03 2017 №2

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

НАДАНО ЧИННОСТІ

Наказ ректора від 30.06.2017 № 101

ВВЕДЕНО У ДІЮ З 01.09 2017 р.

Навчально-методичний відділ

Завідувач _____ Л.С.Любохинець
Підпис Ініціали, прізвище

Хмельницький – 2017

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, що присвоюється	Бакалавр
Назва галузі знань	12 Інформаційні технології
Назва спеціальності	125 Кібербезпека
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
Кваліфікація в дипломі	Ступінь вищої освіти - Бакалавр Спеціальність - 125 Кібербезпека Освітня програма - Кібербезпека
Наявність акредитації	Первинна акредитація планується у 2021 році
Цикл/рівень	Національна рамка кваліфікацій – 7 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 у різних сферах професійної діяльності	
3. Характеристика освітньої програми	
Опис предметної області	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	Акцент на здатності 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. 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 проектів та кваліфікаційної роботи тощо. Поєднуються класичні (пояснювально-ілюстративні, репродуктивні, практичні) та інноваційні (проблемні, проектні, 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 національною 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 проектів, кваліфікаційної роботи тощо.
6. Програмні компетентності	
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	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 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. КЗ 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.
Спеціальні (фахові, предметні) компетентності	КФ 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. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних

	комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 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. Результати навчання	
РН 1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки. РН 2. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. РН 3. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН 4. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. РН 5. 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. РН 6. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. РН 7. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. РН 8. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки. РН 9. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки. РН 10. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. РН 11. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. РН 12. Виконувати аналіз зв'язків між інформаційними процесами на віддалених	

обчислювальних системах.
РН 13. Розробляти моделі загроз та порушника.
РН 14. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН 15. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.
РН 16. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН 17. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН 18. 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.
РН 19. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН 20. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН 21. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН 22. Обирати відповідну технологію програмування, виконати аналіз специфікації задач.
РН 23. Виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування.
РН 24. 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.
РН 25. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.
РН 26. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН 27. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН 28. 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.
РН 29. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
РН 30. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН 31. 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.
РН 32. 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.
РН 33. Здійснювати оцінювання можливості несанкціонованого доступу до елементів

інформаційно-телекомунікаційних систем.
РН 34. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН 35. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН 36. Організовувати процес створення планів неперервності бізнесу.
РН 37. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН 38. 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.
РН 39. Виявляти небезпечні сигнали технічних засобів.
РН 40. 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.
РН 41. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН 42. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН 43. Розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних.
РН 44. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН 45. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем.
РН 46. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки.
РН 47. 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.
РН 48. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН 49. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН 50. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації.
РН 51. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН 52. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН 53. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН 54. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН 55. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

РН 56. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. РН 57. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. РН 58. Відтворювати моральні, культурні, наукові цінності, примножувати досягнення суспільства в соціально-економічній сфері, підтримувати та розвивати фізичне і моральне здоров'я, пропагувати ведення здорового способу життя.	
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 роботи та роботи за фахом.
Матеріально-технічне забезпечення	2 спеціалізовані комп'ютерні лабораторії, оснащені сучасною комп'ютерною та спеціалізованою технікою, спеціалізована лабораторія комплексних систем захисту, спеціалізовані аудиторії університету для проведення практичних і лекційних занять з використанням мультимедійних засобів у відповідності до потреб організації навчального процесу зі спеціальності 125 «Кібербезпека». 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 і практичних робіт; - програма і методичні матеріали для проведення атестації здобувачів
9. Академічна мобільність	
Національна кредитна мобільність	Реалізація національної кредитної мобільності за окремими навчальними модулями, що забезпечують набуття загальних компетентностей
Міжнародна кредитна мобільність	Проходження практик і стажування за кордоном та у представництвах іноземних фірм в Україні на основі двосторонніх договорів між Хмельницьким національним університетом та закладами вищої освіти країн ЄС
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 (роботи), 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	5	іспит	2
ОЗП.03	Фізика	10	іспит	1, 2
ОЗП.04	Англійська мова	5	залік	1, 2
ОЗП.05	Метрологія, вимірювання, стандартизація та сертифікація	4	залік	1
ОЗП.06	Основи теорії кіл, сигнали та процеси в електроніці	4	іспит	3
ОЗП.07	Теорія ймовірності та математична статистика	4	іспит	3
ОЗП.08	Філософія	3	залік	5
ОЗП.09	Громадянське суспільство, економіка та управління	4	залік	6
ОЗП.10	Кібернетичне право	4	залік	7
ОЗП.11	Безпека життєдіяльності, охорона праці, цивільний захист та екологічна безпека	5	іспит	8
ОЗП.12	Культурологія, культура мовлення, етика та естетика	6	залік	8
ОЗП13	Фізичне виховання		залік	2,4
	Разом:	66		
Професійна підготовка (ОПП)				
ОПП.01	Основи інформаційної безпеки	6	залік	1
ОПП.02	Технологія програмування захищених систем	6	іспит	1
ОПП.03	Програмування алгоритмів захисту інформації	12	іспит	3, 4
ОПП.04	Захищені бази даних	5	залік, курсовий проект	3, 4
ОПП.05	Електроніка і схемотехніка систем захисту	9	іспит	4, 5
ОПП.06	Захист інформації в інформаційно-комунікаційних системах	14	іспит, курсовий проект	4, 5
ОПП.07	Безпека Web-ресурсів	5	залік	5
ОПП.08	Стандарти і політики кібербезпеки	5	залік	6
ОПП.09	Прикладна криптологія	5	іспит	6
ОПП.10	Програмні і програмно-апаратні засоби захисту інформаційних систем від несанкціонованого доступу	5	залік	6
ОПП.11	Моделювання систем захисту даних, оцінка ризиків і прийняття рішень	5	іспит	7

Шифр КОП	Компоненти освітньої програми (КОП) (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Семестр
ОПП.12	Комплексні системи захисту інформації: проектування, впровадження, супровід	7	іспит, курсовий проект	7
ОПП.13	Безпека безпроводових і мобільних технологій	5	залік	7
ОПП.14	Управління інформаційною безпекою	5	іспит	7
ОПП.15	Проектно-технологічна практика	5	залік	6
ОПП.16	Переддипломна практика	5	залік	8
ОПП.17	Кваліфікаційна робота	10	кваліфікаційна робота	8
	Разом	114		
Загальний обсяг обов'язкових компонентів		180		
ВИБІРКОВІ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ				
	Вибіркові дисципліни 2 семестру*	12	**	2
	Вибіркові дисципліни 3 семестру*	11	**	3
	Вибіркові дисципліни 4 семестру*	11	**	4
	Вибіркові дисципліни 5 семестру*	12	**	5
	Вибіркові дисципліни 6 семестру*	6	**	6
	Вибіркові дисципліни 7 семестру*	4	**	7
	Вибіркові дисципліни 8 семестру*	4	**	8
Загальний обсяг вибіркових компонентів		**60**		
Загальний обсяг освітньої програми		**240**		

Примітки:

* Перелік вибіркових дисциплін визначається за результатами вільного вибору студентів;

** Кількість іспитів і 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. Щорічно перелік вибіркових освітніх компонент від кожної кафедри оновлюється. Здобувачі вищої освіти за даною ОПП повинні вибрати у кожному з 2-8 семестрів 1-3 дисципліни сумарною кількістю кредитів ЄКТС, що передбачена навчальним планом. Процедура вибору здійснюється у терміни, встановлені відповідним Положенням про порядок вільного вибору навчальних дисциплін студентами Хмельницького національного університету (https://www.khnu.km.ua/root/files/01/06/03/030.pdf).

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 (далі – СВЗЯ) в Університеті відповідає вимогам Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG), статті 16 Закону України «Про вищу освіту» (2014). Створена СВЗЯ функціонує на п'яти організаційних рівнях відповідно до розроблених нормативних документів, що розміщені на вебсайті 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) здійснення моніторингу та періодичного перегляду освітніх програм;
4) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;
5) оприлюднені критерії, правила і процедури оцінювання здобувачів освіти;
6) оприлюднені критерії, правила і процедури оцінювання педагогічної (науково-педагогічної) діяльності педагогічних та науково-педагогічних працівників;
7) оприлюднені критерії, правила і процедури оцінювання управлінської діяльності керівних працівників закладу освіти;
8) забезпечення наявності необхідних ресурсів для організації освітнього процесу, в тому числі для самостійної роботи здобувачів освіти;
9) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;
10) забезпечення наявності інформаційних систем для ефективного управління закладом освіти;
11) створення у закладі освіти інклюзивного освітнього середовища, універсального дизайну та розумного пристосування;
12) 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 результатів навчання відповідними компонентами освітньої програми

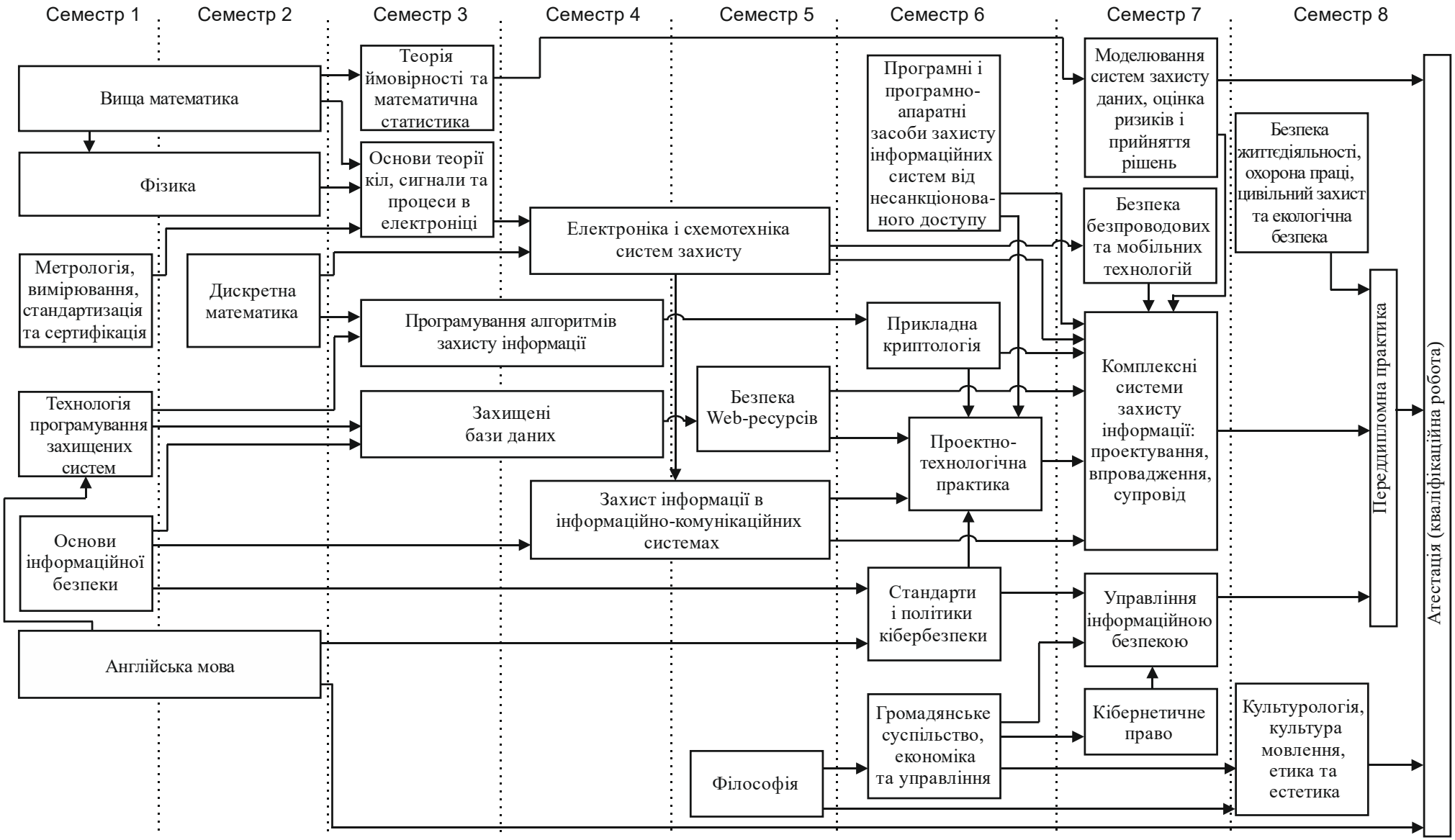
Матриця забезпечення результатів навчання відповідними компонентами освітньої програми представлена в Додатку В.

Використані джерела

1. Закон “Про вищу освіту” [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1556-18.
2. Рівні Національної рамки кваліфікацій [Електронний ресурс]. – Режим доступу: https://mon.gov.ua/ua/osvita/nacionalna-ramka-kvalifikacij/rivni-nacionalnoyi-ramki-kvalifikacij.
3. Про затвердження та введення в дію Методичних рекомендацій щодо розроблення стандартів вищої освіти. Наказ МОНУ № 600 від 01.06.16 року
4. Методичні рекомендації щодо розроблення стандартів вищої освіти. – Затверджено наказом Міністерства освіти і науки України від «01» червня 2016 № 600.
5. Ліцензійні умови провадження освітньої діяльності. Постанова КМУ від 30 грудня 2015 № 1187.
6. Проект стандарту вищої освіти України зі спеціальності 125 – Кібербезпека [Електронний ресурс]. – Режим доступу: https://mon.gov.ua/ua/osvita/visha-osvita/naukovo-metodichna-rada-ministerstva-osviti-i-nauki-ukrayini/proekti-standartiv-vishoyi-osviti.
7. Розроблення освітніх програм. Методичні рекомендації / Авт.: В.М. Захарченко, В.І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. – К. : ДП «НВЦ «Пріоритети», 2014. – 120 с. (Видання здійснено за сприяння проекту Європейського Союзу «Національний Темпус-офіс в Україні»)

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	ОЗП. 12	ОЗП. 13	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
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
КЗ 1	+	+	+	+	+	+	+	+	+	+	+				+	+		+				+					+		+	+
КЗ 2										+				+								+							+	+
КЗ 3				+								+																	+	+
КЗ 4																								+			+		+	+
КЗ 5								+		+							+		+		+				+				+	+
КЗ 6								+	+	+	+	+	+																+	
КЗ 7								+	+			+	+																+	+
КФ1					+					+											+					+	+	+	+	+
КФ2														+		+	+		+	+	+	+	+	+	+	+	+		+	+
КФ 3														+	+	+	+		+	+			+	+	+	+		+	+	
КФ 4																								+			+		+	+
КФ 5																			+					+	+	+		+	+	+
КФ 6														+			+										+	+	+	
КФ 7																									+				+	+
КФ 8										+									+				+				+		+	+
КФ 9																								+	+		+		+	+
КФ 10																+		+				+	+						+	
КФ 11						+													+						+		+	+	+	
КФ 12																	+		+					+	+	+			+	+

Додаток В

VI. Матриця забезпечення програмних результатів навчання (РН) 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	ОЗП. 12	ОЗП. 13	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
РН 1	+	+	+	+	+	+	+	+	+																				
РН 2				+								+																+	+
РН 3																							+			+		+	+
РН 4								+		+							+		+		+				+			+	+
РН 5																							+			+		+	+
РН 6	+	+	+	+		+	+		+	+	+				+	+		+				+					+		+	+
РН 7								+		+		+									+							+	+
РН 8					+					+											+						+	+	+	+
РН 9										+											+						+		+	
РН 10																											+		+	+
РН 11																			+										+	+
РН 12																	+													+
РН 13																							+							+
РН 14																			+						+					+
РН 15														+		+	+						+	+	+	+		+		
РН 16																			+				+			+		+	+	
РН 17																									+					+
РН 18																			+					+					+	
РН 19																							+		+			+	+	
РН 20																+			+			+							+	+
РН 21																							+					+		
РН 22															+	+	+			+										
РН 23															+															
РН 24																									+				+	
РН 25																			+										+	
РН 26																	+		+	+			+			+			+	
РН 27																					+						+		+	+

	ОЗП. 01	ОЗП. 02	ОЗП. 03	ОЗП. 04	ОЗП. 05	ОЗП. 06	ОЗП. 07	ОЗП. 08	ОЗП. 09	ОЗП. 10	ОЗП. 11	ОЗП. 12	ОЗП. 13	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
РН 28																									+				+	
РН 29																			+					+					+	
РН 30																			+						+					+
РН 31																								+	+				+	+
РН 32																								+	+				+	+
РН 33																								+					+	
РН 34														+						+			+			+			+	+
РН 35														+			+										+	+	+	
РН 36									+															+					+	+
РН 37																										+		+	+
РН 38																									+				+	
РН 39						+																			+					
РН 40																									+					
РН 41						+																			+					
РН 42																									+		+		+	
РН 43																			+							+				+
РН 44																			+				+				+			
РН 45																					+			+					+	+
РН 46										+																	+		+	
РН 47																								+			+		+	+
РН 48																								+			+			
РН 49																								+					+	+
РН 50																+		+				+							+	
РН 51																						+	+						+	
РН 52																			+										+	
РН 53																							+					+		
РН 54																			+									+		
РН 55																			+								+	+	+	
РН 56															+								+							
РН 57								+	+	+	+	+	+																+	
РН 58								+	+			+	+																+	+