

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО

Вченою радою ХНЕУ ім. С. Кузнеця
Протокол № 6 від 21.01.2019 р.
Голова Вченої ради

Ректор _____ В. С. Пономаренко

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

РІВЕНЬ ВИЩОЇ ОСВІТИ
СТУПІНЬ ВИЩОЇ ОСВІТИ
ГАЛУЗЬ ЗНАНЬ

Другий (магістерський) рівень
Магістр
12 Інформаційні технології

СПЕЦІАЛЬНІСТЬ

125 “Кібербезпека”

ХАРКІВ, 2019

I. Преамбула

1. РОЗРОБЛЕНО

Методичною комісією Харківського національного економічного університету імені Семена Кузнеця.

Голова методичної комісії:

Пономаренко В.С., д.е.н., проф., ректор ХНЕУ імені С. Кузнеця.

2. ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ

Освітньо-професійна програма другого (магістерського) рівня галузі знань 12 Інформаційні технології, спеціальності 125 “Кібербезпека” затверджена та введена в дію Наказом ректора Харківського національного економічного університету імені Семена Кузнеця від 23.01.2019 р. № 46 у відповідності до рішення вченої ради університету від 21.01.2019 р. Протокол № 6.

3. ВВЕДЕНО ВПЕРШЕ

4. РОЗРОБНИКИ ОПП

Євсеєв Сергій Петрович, доктор технічних наук, завідувач кафедри кібербезпеки та інформаційних технологій

Алексієв Володимир Олегович, доктор технічних наук, професор кафедри кібербезпеки та інформаційних технологій

Шматко Олександр Віталійович, кандидат технічних наук, доцент кафедри кібербезпеки та інформаційних технологій

II. Загальна характеристика

Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 “Кібербезпека”
Освітня програма	“Кібербезпека”
Освітня кваліфікація	Магістр з кібербезпеки за освітньо-професійною програмою “Кібербезпека”
Кваліфікація в дипломі	Магістр з кібербезпеки за освітньо-професійною програмою “Кібербезпека”
Опис предметної області	Об’єкти вивчення: об’єкти інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення складових безпеки інформації: інформаційна безпека, кібербезпека, безпека інформації; процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту; теоретичні та правові основи використання, принципи функціонування блокчейн технологій, обігу криптовалют. Цілі навчання: підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки, які володіють механізмами забезпечення безпеки в децентралізованих системах, ефективними засобами обмежень ризиків створення та використання криптовалют, використання смартконтрактів. Теоретичний зміст предметної області: принципи формування систем забезпечення інформаційної та/або кібербезпеки; методи та засоби виявлення, управління та ідентифікації ризиків; загальні принципи та правила застосування криптографічних способів у блокчейн технології, методологічні основи розробки та функціонування блокчейн платформ, смартконтрактів, методи та механізми забезпечення безпеки в сучасних системах цифровій економіки. Методи, методики та технології: статистичні, якісні та кількісні методи/ методики оцінки поточного стану інформаційної безпеки; експертного оцінювання, математичного моделювання, прогнозування; інформаційно-комунікаційні технології, спеціальне програмне забезпечення; методи дослідницької діяльності та презентації результатів. Інструменти та обладнання: сучасне інформаційно-

	комунікаційне обладнання, Security Information and Event Management системи та програмні продукти: управління інформаційною безпекою (Security Information Management), та управління подіями безпеки (Security Event Management).
Академічні права випускників	Можливість продовження навчання на третьому (освітньо-науковому) рівні (доктор філософії) за спеціальністю “Кібербезпека”; отримання післядипломної освіти на споріднених та інших спеціальностях; підвищення кваліфікації.
Працевлаштування випускників	Магістр з кібербезпеки може працювати керівником підприємств, установ та організацій, керівним працівником апарату місцевих органів державної влади; керівником фінансових, бухгалтерських, економічних, юридичних та адміністративних підрозділів та інші керівники; керівником підрозділів комп’ютерних послуг; керівником проєктів та програм; менеджером (управителем) систем з інформаційної безпеки; розробником комп’ютерних програм; викладачем університетів та вищих навчальних закладів; науковим співробітником (інформаційна аналітика); професіоналом в галузі інформації та інформаційні аналітики; науковим співробітником (електроніка, телекомунікації, проєкти та програми), професіоналом з управління проєктами та програмами

III. Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Обсяг освітньо-професійної програми підготовки магістра галузі знань 12 “Інформаційні технології” за освітньо-професійною програмою “Кібербезпека” спеціальності 125 “Кібербезпека” (бакалавр) – 90 кредитів ЄКТС.

Термін навчання:

денна форма – один рік 4 місяці;

заочна форма – один рік 4 місяці.

Обсяг кредитів ЄКТС для здобуття ступеня магістра зі спеціальності 125 Кібербезпека освітньо-професійна програма “Кібербезпека”

Цикли підготовки	Кількість кредитів ECTS
Освітньо-професійна програма магістра за циклами:	90
Цикл професійної підготовки	90
у т. ч.	
базові навчальні дисципліни	45 (50 %)
вибіркові навчальні дисципліни	45 (50 %)

Вибіркова складова освітньо-професійної програми складається з:

МАГ-МАЙНОР – умовна назва вибірових дисциплін із загального переліку Університету (загальноуніверситетський пул) для освітньо-кваліфікаційного рівня магістр. Дисципліни **МАГ-МАЙНОР** є обов’язковими для вибору студентами і входять до загального обсягу кредитів ЄКТС за освітньо-професійною програмою підготовки магістрів.

Ідея дисциплін **МАГ-МАЙНОР** полягає у вільному виборі студентами магістратури дисциплін таких напрямків, які відображають його інтереси, вподобання та плани на майбутнє працевлаштування. Взяти участь у **МАГ-МАЙНОР** можуть усі факультети і кафедри університету. Індивідуальний план студента буде формуватися з найкращих на його думку навчальних дисциплін.

Загальний обсяг **МАГ-МАЙНОР** складає 20 кредитів ЄКТС (по 5 кредитів на дисципліну):

КОМПЛЕКСНИЙ ТРЕНІНГ. Головною метою комплексного тренінгу є формування у студентів навичок прийняття послідовних рішень щодо вибору механізмів забезпечення безпеки в сучасних обчислювальних мережах і системах, методів криптоаналізу щодо визначення рівня стійкості обраних криптосистем.

IV. Перелік компетентностей випускника

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ-1. Здатність до професійного спілкування іноземною мовою. КЗ-2. Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях. КЗ-3. Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням.
Спеціальні (фахові, предметні) компетентності	КФ-1. Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації. КФ-2. Здатність до виявлення уразливостей та забезпечення безпеки дротових і бездротових мереж, розслідування інцидентів інформаційної та/або кібербезпеки, протидії зловмисному програмному забезпеченню. КФ-3. Здатність до забезпечення безпеки Web-ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження. КФ-4. Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки. КФ-5. Здатність до забезпечення безпеки інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації. КФ-6. Здатність до забезпечення безпеки інформації, що обробляється в центрах сертифікації ключів, здійснення адміністрування таких систем та обслуговування. КФ-7. Здатність до забезпечення безпеки інформації в апаратних засобах на різних платформах. КФ-8. Володіння знаннями про принципи застосування криптографічних методів у блокчейн технологіях, здатність розробки, кодування, розгортання і виконання комплексних децентралізованих додатків (Dapps). КФ-9. Володіння знаннями про принципи розробки, кодування, розгортання і виконання розумних (смарт) контрактів – обчислювального елементу технології блокчейн.

З метою забезпечення кореляції визначених компетентностей з класифікацією компетентностей НРК використовується матриця відповідності визначених компетентностей та дескрипторів НРК, яка є інформаційним додатком (Таблиця 1 Пояснювальної записки).

**V. Нормативний зміст підготовки здобувачів вищої освіти,
сформульований у термінах результатів навчання за спеціальністю
125 “Кібербезпека” освітньо-професійна програма “Кібербезпека”**

Результати навчання	ПРН-1 Знання законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності
	ПРН-2 Знання принципів формування систем забезпечення інформаційної та/або кібербезпеки
	ПРН-3 Знання принципів забезпечення безпеки у мережевих пристроях
	ПРН-4 Знання теорії децентралізованих систем управління на основі блокчейн технології
	ПРН-5 Знання методів та засобів виявлення, управління та ідентифікації ризиків
	ПРН-6 Знання методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації
	ПРН-7 Знання методів та засобів технічного та криптографічного захисту інформації
	ПРН-8 Вміння готувати пропозиції до нормативних актів щодо забезпечення складових безпеки: інформаційної безпеки, кібербезпеки, безпеки інформації в сучасних обчислювальних мережах і системах
	ПРН-9 Знання моделей безпеки, принципів їх використання в сучасних обчислювальних мережах і системах
	ПРН-10 Засвоєння принципів та правил застосування криптографічних способів у блокчейн технологіях
	ПРН-11 Засвоєння методологічних основ розробки та функціонування блокчейн платформ
	ПРН-12 Набуття реалізаційних здатностей з використання криптовалют та функціонування смартконтрактів
	ПРН-13 Оволодіння ефективними засобами обмежень ризиків створення та використання криптовалют, використання смартконтрактів
	ПРН-14 Здатність проводити наукові дослідження під керівництвом наукового керівника
	ПРН-15 Здатність планувати та проводити експериментальні дослідження з метою визначення оцінки ефективності функціонування комплексної системи захисту інформації

СТРУКТУРА ПРОГРАМИ ПІДГОТОВКИ МАГІСТРІВ

Галузь знань 12 “Інформаційні технології”,
спеціальність 125 “Кібербезпека”
освітньо-професійна програма “Кібербезпека”

Складові освітньо-професійної програми	Загальна кількість		Форма контролю
	кредитів ЄКТС	годин	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
БАЗОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ			
РИЗИК-МЕНЕДЖМЕНТ	5	150	Екзамен
ІНОЗЕМНА МОВА: АКАДЕМІЧНЕ ПИСЬМО	4	120	Залік
МЕТОДОЛОГІЇ НАУКОВИХ ДОСЛІДЖЕНЬ	4	120	Залік
КОНСУЛЬТАЦІЙНИЙ ПРОЕКТ	1	30	Курсова робота
КОМПЛЕКСНИЙ ТРЕНІНГ "КРИПТОГРАІЯ І КРИПТОАНАЛІЗ"	3	90	Звіт
НАУКОВО-ДОСЛІДНА ПРАКТИКА	1	30	Звіт
ПЕРЕДДИПЛОМНА ПРАКТИКА	8	240	Звіт
ДИПЛОМНИЙ ПРОЕКТ	19	570	Дипломний проект
ВСЬОГО БАЗОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ:	45	1350	
ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ			
Студенти обирають один із запропонованих мейджорів			
Мейджор “Інформаційна безпека”			
ЕТІЧНИЙ ХАКІНГ	5	150	Екзамен
ДАТА-САЙНС: НАУКА О ДАНИХ	5	150	Екзамен
АДМІНІСТРУВАННЯ, АУДИТ ТА БЕЗПЕКА У РОЗПОДІЛЕНИХ СИСТЕМАХ	5	150	Екзамен
ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У МЕРЕЖЕВИХ ПРИСТРОЯХ	5	150	Екзамен
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	5	150	Екзамен
Мейджор “Інтелектуальні системи і блокчейн технології”			
ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ	5	150	Екзамен
ПРАКТИЧНІ ЗАСТОСУНКИ У КРИПТОГРАФІЇ	5	150	Екзамен
БЛОКЧЕЙН: МАТЕМАТИЧНІ ПРОБЛЕМИ ТА ЗАСТОСУНКИ	5	150	Екзамен
ДЕЦЕНТРОЛІЗОВАНІ ЗАСТОСУНКИ	5	150	Екзамен
СМАРТ-КОНТРАКТИ	5	150	Екзамен
Вибір навчальних дисциплін здійснюється із загальноуніверситетського пулу			
МАГ-МАЙНОР	5	150	Залік
МАГ-МАЙНОР	5	150	Залік
МАГ-МАЙНОР	5	150	Залік
МАГ-МАЙНОР	5	150	Залік
ВСЬОГО ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ:	45	1350	
ЗАГАЛЬНА КІЛЬКІСТЬ:	90	2700	

VI. Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація за спеціальністю здійснюється екзаменаційною комісією відповідно до вимог стандарту вищої освіти після виконання студентом навчального плану у формі: публічного захисту кваліфікаційної роботи магістра за спеціальністю 12 Інформаційні технології, освітньо-професійною програмою “Кібербезпека”(денна форма) або єдиного кваліфікаційного іспиту за спеціальністю у порядку, визначеному Кабінетом Міністрів України (заочна форма). До атестації допускаються студенти, які виконали всі вимоги освітньої програми та навчального плану. Результати атестації визначаються оцінками за національною шкалою: “відмінно”, “добре”, “задовільно”, “незадовільно”.
Вимоги до заключної кваліфікаційної роботи	Харківський національний економічний університет імені Семена Кузнеця розробляє та затверджує: 1) положення про Екзаменаційну комісію (ЕК); 2) порядок перевірки кваліфікаційних дипломних магістерських робіт на плагіат; 3) нормативи унікальності текстів кваліфікаційних дипломних магістерських робіт. Атестація осіб, які здобувають ступінь магістра, здійснюється ЕК, до складу якої можуть включатися представники роботодавців та їх об'єднань. Атестація здійснюється відкрито і публічно. Дипломна робота магістра допускається до захисту перед ЕК за умови, якщо рівень її унікальності (оригінальності) відповідає нормативу, який офіційно затверджений Харківським національним економічним університетом імені Семена Кузнеця. Вимоги до заключної кваліфікаційної роботи: Кваліфікаційна дипломна магістерська робота – це навчально-наукова робота студента, яка виконується на завершальному етапі здобуття кваліфікації магістра з кібербезпеки для встановлення відповідності отриманих здобувачами вищої освіти результатів навчання (компетентностей) вимогам стандартів вищої освіти. Вона є кваліфікаційним документом, на підставі якого ЕК визначає рівень теоретичної підготовки випускника, його готовність до самостійної роботи за фахом і приймає рішення щодо присвоєння відповідної кваліфікації та видачу диплома. Дипломна робота магістра є інструментом закріплення та демонстрації сформованих упродовж навчання загальних та спеціальних компетентностей відповідно профілю обраної освітньо-професійної програми. Для оприлюднення та публічного ознайомлення зі змістом кваліфікаційних робіт, запобігання академічного плагіату дипломні роботи мають бути розміщені на офіційному сайті Харківського національного економічного університету імені Семена Кузнеця.
Вимоги до публічного захисту (демонстрації за наявності)	У процесі публічного захисту кандидат на присвоєння магістерського ступеня повинен показати уміння чітко і упевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь студента повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду.

	Ухвалення екзаменаційною комісією рішення про присудження ступеня магістра економіки та видачу диплома магістра за результатами підсумкової атестації студентів оголошуються після оформлення в установленому порядку протоколів засідань екзаменаційної комісії.
Вимоги до кваліфікаційного екзамену	Кваліфікаційний екзамен має передбачати оцінювання обов'язкових результатів навчання, визначених цим стандартом та освітньо-професійною програмою.

VII. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Визначаються відповідно до Європейських стандартів та рекомендацій щодо забезпечення якості вищої освіти (ESG) та статті 16 Закону України “Про вищу освіту”.

Принципи та процедури забезпечення якості освіти	Принципи забезпечення якості освіти: • відповідальність за якість вищої освіти, що надається; • забезпечення якості відповідає різноманітності систем вищої освіти, закладів вищої освіти, програм і студентів; • забезпечення якості сприяє розвитку культури якості; • забезпечення якості враховує потреби та очікування студентів, усіх інших стейкхолдерів та суспільства. Процедурами забезпечення якості освіти є: • розробка стратегії і політики в сфері якості вищої освіти; • розробка механізму формування, затвердження, моніторингу та періодичного перегляду освітньо-професійних програм; • розробка системи оцінювання знань здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярного оприлюднення результатів таких оцінювань на офіційному веб-сайті ХНЕУ ім. С. Кузнеця, на інформаційних стендах та в будь-який інший спосіб, згідно з розробленими та затвердженими правилами. • організація підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; • формування необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньо-професійною програмою; • створення та функціонування інформаційних систем для ефективного управління освітнім процесом; • оприлюднення об'єктивної неупередженої інформації про освітньо-професійні програми, ступені вищої освіти та кваліфікації; • розробка політики щодо ефективної системи запобігання та виявлення академічного плагіату у наукових працях здобувачів вищої освіти; • інших процедур і заходів.
Моніторинг та періодичний перегляд освітніх програм	Здійснюється моніторинг і періодичний перегляд програм з метою забезпечення їх відповідності потребам студентів і суспільства. Моніторинг спрямований на безперервне вдосконалення програм. Про будь-які дії, заплановані або вжиті як результат перегляду, слід інформувати всі зацікавлені сторони. Регулярний моніторинг, перегляд і оновлення освітніх програм мають на меті гарантувати відповідний рівень надання освітніх послуг, а також створює сприятливе й ефективне навчальне середовище для здобувачів

	вищої освіти. Це передбачає оцінювання: • змісту програми в контексті останніх досліджень у сфері кібербезпеки, гарантуючи відповідність програми сучасним вимогам; • потреб суспільства, що змінюються; • навчального навантаження здобувачів вищої освіти, їх досягнень і результатів завершення освітньо-професійної програми; • ефективності процедур оцінювання студентів; • очікувань, потреб і задоволеності здобувачів вищої освіти змістом та процесом навчання; • навчального середовища відповідності меті і змісту програми; якості сервісних послуг для здобувачів вищої освіти.
Програми регулярно переглядають і оновлюють, залучаючи до цього процесу здобувачів вищої освіти, роботодавців та інших стейкхолдерів.	
Щорічне оцінювання здобувачів вищої освіти	Оцінювання здобувачів вищої освіти базується на принципах студентоцентрованого навчання та передбачає наступне: • оцінювачі (експерти) ознайомлені з існуючими методами проведення тестування та екзаменування і отримують підтримку для розвитку власних навичок у цій сфері; • критерії та методи оцінювання, а також критерії виставлення оцінок оприлюднюються заздалегідь; • оцінювання здобувачів вищої освіти дозволяє продемонструвати ступінь досягнення ними запланованих результатів навчання; • оцінювання проводиться предметною комісією у складі більше ніж дві особи; • процедури оцінювання здобувачів вищої освіти повинні враховувати пом'якшувальні обставини; • оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених процедур; • наявність офіційної процедури розгляду апеляцій здобувачів вищої освіти.
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Система підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників розробляється у відповідності до діючої нормативної бази та будується на наступних принципах: • обов'язковості та періодичності проходження стажування і підвищення кваліфікації; • прозорості процедур організації стажування та підвищення кваліфікації; • моніторингу відповідності змісту програм підвищення кваліфікації задачам професійного діяльності; • обов'язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; • оприлюднення результатів стажування та підвищення кваліфікації.
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Система підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників розробляється у відповідності до діючої нормативної бази та будується на наступних принципах: • обов'язковості та періодичності проходження стажування і підвищення кваліфікації; • прозорості процедур організації стажування та підвищення кваліфікації; • моніторингу відповідності змісту програм підвищення кваліфікації задачам професійного діяльності; • обов'язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; • оприлюднення результатів стажування та підвищення кваліфікації.

Наявність необхідних ресурсів для організації освітнього процесу	Вищі навчальні заклади забезпечують освітній процес необхідними та доступними для здобувачів вищої освіти ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснюють відповідну підтримку студентів. При плануванні, розподілі та наданні навчальних ресурсів і забезпеченні підтримки здобувачів вищої освіти враховуються потреби різноманітного студентського контингенту (такого як студенти: з досвідом, заочної форми навчання, працюючі, іноземні, з особливими потребами) та принципи студентоцентрованого навчання. Внутрішнє забезпечення якості освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а студенти поінформовані про їх наявність.
Наявність інформаційних систем для ефективного управління освітнім процесом	З метою управління освітніми процесами розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну систему управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної кампанії, планування та організація навчального процесу; доступ до навчальних ресурсів; обліку та аналізу успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; моніторинг дотримання стандартів якості; управління знаннями та інноваційний менеджмент; управління кадрами та ін.
Публічність інформації про освітні програми, ступені вищої освіти та кваліфікації	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація про діяльність за спеціальністю 125 "Кібербезпека" публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних здобувачів вищої освіти, студентів, випускників, інших стейкхолдерів і громадськості. Надається інформація про освітню діяльність за спеціальністю 125"Кібербезпека", включаючи програми, критерії відбору на навчання; заплановані результати навчання за цими програмами; кваліфікації; процедури навчання, викладання та оцінювання, що використовуються; прохідні бали та навчальні можливості, доступні для студентів тощо.
Запобігання та виявлення академічного плагіату	Система забезпечення дотримання академічної доброчесності учасниками освітнього процесу, сформована в ХНЕУ ім. С. Кузнеця, базується на таких принципах: дотримання загальноприйнятих принципів моралі; демонстрація поваги до Конституції і законів України і дотримання їхніх норм; повага до всіх учасників освітнього процесу незалежно від їхнього світогляду, соціального стану, релігійної та національної приналежності; дотримання норм законодавства про авторське право; посилення на джерела інформації у разі запозичень ідей, тверджень, відомостей; самостійне виконання індивідуальних завдань. У випадку порушення принципів академічної доброчесності відповідні особи притягуються до відповідальності відповідно до законодавства та діючих у ХНЕУ ім. С. Кузнеця положень та норм.

Спеціальні вимоги до зарахування: Набір на спеціальність освітнього рівня “магістр” здійснюється на загальних умовах вступу за результатами фахового випробування:

- 1) з іноземної мови за результатами незалежного зовнішнього тестування;
- 2) за комплексом навчальних дисциплін з галузі знань 12 “Інформаційні технології” та з урахуванням середнього балу документа про вищу освіту першого (бакалаврського) рівня.

Для успішного засвоєння освітньо-професійної програми магістра абітурієнти повинні мати перший (бакалаврський) рівень вищої освіти (диплом бакалавра), підтверджений документом державного зразка, що виданий закладом вищої освіти III-IV рівня акредитації.

Профіль програми: інтелектуальні системи і блокчейн технології

Ключові результати навчання за освітньо-професійною програмою “Кібербезпека”:

- законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;
- принципів формування систем забезпечення інформаційної та/або кібербезпеки;
- принципів забезпечення безпеки у мережевих пристроях;
- теорії децентралізованих систем управління на основі блокчейн технології;
- 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.

Професійні профілі випускників: магістр здатний виконувати професійні роботи (за Державним класифікатором професій ДК 003: 2010):

- 1210.1 Керівники підприємств, установ та організацій;
- 1229.3 Керівні працівники апарату місцевих органів державної влади;
- 1231 Керівники фінансових, бухгалтерських, економічних, юридичних та адміністративних підрозділів та інші керівники;
- 1236 Керівники підрозділів комп’ютерних послуг;
- 1238 Керівники проектів та програм;
- 1495 Менеджери (управителі) систем з інформаційної безпеки;
- 2132.2 Розробники комп’ютерних програм;
- 231 Викладачі університетів та вищих навчальних закладів;
- 2433.1 Наукові співробітники (інформаційна аналітика);
- 2433.2 Професіонали в галузі інформації та інформаційні аналітики;
- 2144.1 Наукові співробітники (електроніка, телекомунікації);
- 2144.2 Інженери в галузі електроніки та телекомунікацій;
- 2447.1 Наукові співробітники (проекти та програми);
- 2447.2 Професіонали з управління проектами та програмами.

VIII. Перелік нормативних документів, на яких базується освітньо-професійна програма

Освітня діяльність Харківського національного економічного університету ім. С. Кузнеця ґрунтується на концептуальних засадах Національної Доктрини розвитку освіти, Державній Національній програмі “Освіта” (“Україна XXI століття”), Законі України “Про освіту”, Законі України “Про вищу освіту”, наказах Міністерства освіти і науки, Статуті Харківського національного економічного університету ім. С. Кузнеця, Тимчасовому Положенні “Про організацію освітнього процесу в Харківському національному економічному університеті імені Семена Кузнеця”, затвердженому Вченою радою університету 21.12.2015 року протокол № 6, Тимчасовому Положенні “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою”, затвердженому Вченою радою університету 30.08.2013 року протокол № 1, Правилах розпорядку Університету та інших нормативно-правових актах.

Перелік використаних джерел

1. Закон “Про вищу освіту” – <http://zakon4.rada.gov.ua/laws/show/1556-18>.
2. Національний класифікатор України: “Класифікатор професій” ДК 003:2010.– К. : Видавництво “Соцінформ”, 2010. – 746 с.
3. Національна рамка кваліфікацій – <http://zakon4.rada.gov.ua/laws/show/1341-2011-п>.
4. Перелік галузей знань і спеціальностей – <http://zakon4.rada.gov.ua/laws/show/266-2015-п>.
5. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти – <file:///D:/Users/Dell/Downloads/BolonskyiProcessNewParadigmHE.pdf>.
6. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – http://ihed.org.ua/images/biblioteka/Rozvitok_sisitemi_zabesp_yakosti_VO_UA_2015.pdf.
7. Розроблення освітніх програм: методичні рекомендації – http://ihed.org.ua/images/biblioteka/rozroblennya_osv_program_2014_tempus-office.pdf.
8. 2015 р. Європейська кредитна трансферно-накопичувана система - Довідник користувача (переклад українською мовою) <http://erasmusplus.org.ua/erasmus/ka3-pidtrymka-reform/natsionalna-komanda-ekspertiv-here/materiali-here.html>

Пояснювальна записка

Матриця відповідності визначених Стандартом компетентностей дескрипторам НРК та матриця відповідності визначених Стандартом результатів навчання та компетентностей представлені в Таблицях 1 і 2.

Таблиця 1

Матриця відповідності визначених компетентностей дескрипторам НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
КЗ-1. Здатність до професійного спілкування іноземною мовою	+	+	+	+
КЗ-2. Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях	+	+	+	+
КЗ-3. Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням	+	+	+	+
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
КФ-1. Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації	+	+		
КФ-2. Здатність до виявлення уразливостей та забезпечення безпеки дротових і бездротових мереж, розслідування інцидентів інформаційної та/або кібербезпеки, протидії злоякісному програмному забезпеченню	+	+		
КФ-3. Здатність до забезпечення безпеки Web-ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження	+	+		
КФ-4. Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки	+	+		+
КФ-5. Здатність до забезпечення безпеки інформації, що	+	+	+	

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації				
КФ-6. Здатність до забезпечення безпеки інформації, що обробляється в центрах сертифікації ключів, здійснення адміністрування таких систем та обслуговування	+	+		+
КФ-7. Здатність до забезпечення безпеки інформації в апаратних засобах на різних платформах	+	+		+
КФ-8. Володіння знаннями про принципи застосування криптографічних методів у блокчейн технологіях, здатність розробки, кодування, розгортання і виконання комплексних децентралізованих додатків (Dapps).	+	+		+
КФ-9. Володіння знаннями про принципи розробки, кодування, розгортання і виконання розумних (смарт) контрактів — обчислювального елементу технології блокчейн.	+	+		+

Таблиця 2

Матриця відповідності визначених Стандартом результатів навчання та компетентностей

програмні результати навчання	компетентності												
	інтег- ральна	загальні		спеціальні (фахові)									
		КЗ-1	КЗ-2	КЗ-3	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9
ПРН-1 Знання законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності	+		+			+	+					+	+
ПРН-2 Знання принципів формування систем забезпечення інформаційної та/або кібербезпеки	+	+		+	+				+				
ПРН-3 Знання принципів забезпечення безпеки у мережових пристроях	+	+		+				+					
ПРН-4 Знання теорії децентралізованих систем управління на основі блокчейн технології	+	+		+						+			
ПРН-5 Знання методів та засобів виявлення, управління та ідентифікації ризиків	+	+	+	+									
ПРН-6 Знання методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації	+	+	+	+									
ПРН-7 Знання методів та засобів технічного та криптографічного захисту інформації	+	+	+		+			+	+			+	+
ПРН-8 Вміння готувати пропозиції до нормативних актів щодо забезпечення складових безпеки: інформаційної безпеки, кібербезпеки, безпеки інформації в сучасних обчислювальних мережах і системах	+	+	+	+	+	+	+	+					
ПРН-9 Знання моделей безпеки, принципів їх використання в сучасних обчислювальних мережах і системах	+			+		+							
ПРН-10 Засвоєння принципів та правил застосування криптографічних способів у блокчейн технологіях	+	+			+		+		+	+	+	+	+

програмні результати навчання	компетентності												
	інтег- ральна	загальні		спеціальні (фахові)									
		КЗ-1	КЗ-2	КЗ-3	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9
ПРН-11 Засвоєння методологічних основ розробки та функціонування блокчейн платформ	+								+	+	+	+	+
ПРН-12 Набуття реалізаційних здатностей з використання криптовалют та функціонування смартконтрактів	+	+	+							+	+	+	+
ПРН-13 Оволодіння ефективними засобами обмежень ризиків створення та використання криптовалют, використання смартконтрактів	+	+		+		+			+	+	+	+	+
ПРН-14 Здатність проводити наукові дослідження під керівництвом наукового керівника	+	+	+	+	+	+	+	+		+	+	+	+
ПРН-15 Здатність планувати та проводити експериментальні дослідження з метою визначення оцінки ефективності функціонування комплексної системи захисту інформації	+	+	+	+	+	+	+	+					