МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет міського господарства імені О.М. Бекетова

ПРОЄКТ

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Кібербезпека об'єктів критичної інфраструктури»

Рівень вищої освіти перший (бакалаврський) рівень

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека та захист інформації

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Голова вченої ради

Володимир БАБАЄВ

(протокол № ____ від «_____»_____ 2024 р.)

Освітня програма вводиться в дію з ____.____.2024 р.

(наказ № ____ від «_____»_____ 2024 р.)

2024 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної/наукової програми

Освітню програму розглянуто і схвалено:

Кафедра Систем електропостачання та електроспоживання міст

Протокол № ____ від «_____»_____ 2024 р.

Вчена рада Навчально-наукового інституту енергетичної, інформаційної та транспортної інфраструктури

Протокол № ____ від «_____»_____ 2024 р.

Науково-методична рада ХНУМГ ім. О.М. Бекетова

Протокол № ____ від «_____»_____ 2024 р.

ПЕРЕДМОВА

Розроблено членами групи забезпечення освітньої програми «Кібербезпека об’єктів критичної інфраструктури» першого (бакалаврського) рівня спеціальності 125 Кібербезпека та захист інформації на кафедрі систем електропостачання та електроспоживання міст Харківського національного університету міського господарства імені О.М. Бекетова

Ім’я, прізвище гаранта освітньої програми та інших розробників	Науковий ступінь, вчене звання, посада	Підпис
Аксьонов Євген Олександрович гарант	к.т.н., доцент каф. автоматизації та комп'ютерно-інтегрованих технологій	
Булаєнко Марина Володимирівна	к.т.н., доцент каф. комп’ютерних наук	
Плюгін Владислав Євгенович	д.т.н., проф., завідувач кафедри систем електропостачання та електроспоживання міст	

При розробці освітньої програми враховані вимоги:

- стандарту вищої освіти України спеціальності 125 Кібербезпека за першим (бакалаврським) рівнем, затвердженим наказом від 04.10.2018 р. № 1074

Рецензенти:

1. НЕК «Укренерго»
2. Huawei Україна
3. НАН України

1. Профіль освітньої програми Кібербезпека об’єктів критичної інфраструктури зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Повна назва закладу вищої освіти	Харківський національний університет міського господарства імені О.М. Бекетова
Рівень вищої освіти	Перший (бакалаврський)
Освітня та професійна кваліфікація (у разі присвоєння)	бакалавр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека об’єктів критичної інфраструктури
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС
Форма (и) здобуття освіти	денна
Наявність акредитації	*Акредитація не проводилась*
Цикл/рівень	Перший (бакалаврський) рівень НРК України – 6 рівень FQ-EHEA – перший цикл EQF-LLL – 6 рівень
Вимоги до рівня освіти осіб, які можуть розпочати навчання за програмою	Наявність повної загальної середньої освіти /наявність освітньо-кваліфікаційного рівня молодший спеціаліст («молодший бакалавр», «фаховий бакалавр»)
Мова(и) викладання	Українська
Інтернет-адреса постійного розміщення опису освітньої програми	https://eog.kname.edu.ua/osvitni-prohramy/bakalavr/kiberbezpeka
2 – Цілі освітньої програми	
	Підготовка фахівців, здатних працювати у сфері забезпечення захисту об’єктів критичної інфраструктури, які володіють всебічним досвідом як технічних, так і міжособистісних навичок відповідно до місії та стратегії університету, яка полягає у підготовці висококваліфікованих кадрів для регіонального розвитку та міського господарства.
3 - Характеристика освітньої програми	
Предметна область	*Об’єкти вивчення та діяльності:* – об’єкти інформатизації підприємств електроенергетичного комплексу, електротехнічні та електромеханічні служби організацій, 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 електроенергетики, що підлягають захисту.

	Ціль навчання: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, зокрема для об'єктів критичної інфраструктури *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.
Тип освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Здобувачі вищої освіти за цією освітньо-професійною програмою мають можливість набути загальних знань і професійних навичок у сфері кібернетичного захисту інформації. *Ключові слова*: кібербезпека, комп'ютерні мережі, програмування, інформаційно-комунікаційні технології, електроенергетичні, захист інформації, пристрої та устаткування, системи керування, передачі та розподілу електричної енергії, математичне моделювання.
Особливості програми	Особливості освітньої програми полягають у підготовці фахівців, здатних використовувати і впроваджувати технології інформаційної та / або кібербезпеки в галузях критичної інфраструктури, зокрема у галузі електропостачання та видобутку електричної енергії з використанням спеціалізованого комплексу на базі унікальної цифрової підстанції, яка поєднує як апаратну так і програмну частини. До викладання залучені іноземні та вітчизняні фахівці галузі з діючих об'єктів із забезпечення кібербезпеки, викладання окремих освітніх компонентів англійською мовою.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може працювати в підрозділах великих підприємств та установ як сфери електроенергетики, так і інших структурах,

	забезпечуючи захист комп'ютерних систем та мереж, здійснювати забезпечення захищеної об'єктів інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; Професії, професійні назви робіт (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (ДК 003:2010): 3439 Фахівець із організації інформаційної безпеки; 3439 Фахівець із організації захисту інформації з обмеженим доступом; 3439 (24771). Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO-08); 3113. Фахівець з енергетичного менеджменту.
Академічні права випускників	Можливість продовження навчання на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти, підвищення кваліфікації.
5 – Викладання та оцінювання	
Викладання та навчання	Студенто-центроване навчання, проблемно-орієнтоване навчання, лекції, практичні заняття, лабораторні роботи, самостійна робота, консультації, проєктна робота, підготовка кваліфікаційної роботи. Методи навчання: проблемного викладу, ілюстрації та демонстрації, частково-пошуковий, дослідницький, практичний.
Оцінювання	Поточний контроль: усне та письмове опитування, тести, презентації індивідуальних завдань. Підсумковий контроль: письмові екзамени і диференційовані заліки, захист курсових робіт та звітів з практики. Атестація: публічний захист кваліфікаційної роботи.
6 – Компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки об'єктів електроенергетики, що характеризується 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
Спеціальні (фахові,	**ФК 1.** Здатність застосовувати законодавчу та нормативноправову

предметні) компетентності (ФК)	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 інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. **ФК 3.** Здатність до використання програмних та програмноапаратних 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	
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.ч: 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 та\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 ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризико-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.

	ПРН 55. Знати і розуміти принципи роботи електричних систем та мереж, силового обладнання електричних станцій та підстанцій, пристроїв захисного заземлення та грозозахисту та уміти використовувати їх для вирішення практичних проблем у професійній діяльності. **ПРН 56.** Знати і розуміти теоретичні основи метрології та електричних вимірювань, принципи роботи пристроїв автоматичного керування, релейного захисту та автоматики, мати навички здійснення відповідних вимірювань і використання зазначених пристроїв для вирішення професійних завдань.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Усі науково-педагогічні працівники мають кваліфікацію відповідно освітніх компонент, досвід практичної та науково-педагогічної діяльності, регулярно підвищують свою кваліфікацію через участь у наукових проєктах, конференціях, стажування в закладах та підприємствах України.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення освітньої програми відповідає вимогам та забезпечує можливість ефективної підготовки здобувачів. Навчальний процес у повному обсязі забезпечений аудиторним фондом, адміністративними і допоміжними приміщеннями. Для забезпечення лабораторного практикуму створено та успішно функціонують 4 спеціалізовані лабораторії, які повністю відповідають сучасним вимогам. Лабораторія «Віртуальна підстанція» на апаратній базі Siemens/ABB та серверної станції дозволяє опановувати навички як із забезпечення кіберзахисту об'єктів електроенергетики, так і імітувати потенційні загрози. Лабораторія створена сумісно з фірмами Schneider Elektrik та ABB для дослідження та вивчення основних сучасних моделей комутаційної апаратури. Лабораторія «Цифрових пристроїв та релейного захисту», «Електричних станцій та підстанцій», створена разом з АТ «Харківобленерго» для вивчення та практичної реалізації сучасних цифрових пристроїв в електричних мережах та вивчення основних технічних характеристик електричного обладнання з метою раціонального його використання. Навчальний процес з усіх дисциплін забезпечений засобами наочності (презентації до лекційного матеріалу, плакати, схеми, таблиці, макети, зразки, тощо), необхідним технічним і технологічним обладнанням.
Інформаційне та навчально-методичне забезпечення	Усі освітні компоненти забезпечені навчально-методичними матеріалами, розміщеними у відповідних курсах на платформі дистанційного навчання Moodle. Здобувачі мають вільний доступ: - до сучасної фахової літератури та періодичних видань; баз даних Scopus та Web of Science; ресурсів Springer; бази даних Science Direct від видавництва Elsevier; - до міжнародних платформ дистанційного навчання (Cursera, Udemy, Labster, FutureLearn); - до ресурсів онлайн-платформи UkraineGlobalFaculty. Усі навчально-методичні матеріали доступні для здобувачів у читальних залах наукової бібліотеки http://library.kname.edu.ua/index.php/uk/, в тому числі у залі

	інформаційного сервісу, обладнаному комп'ютерами з доступом до мережі Інтернет та локальної мережі Університету, у цифровому репозиторії http://eprints.kname.edu.ua, на порталах Центру дистанційного навчання https://dl.kname.edu.ua/. Для перевірки на ознаки плагіату використовують системи Unichek, StrikePlagiarism.
9 – Академічна мобільність	
Національна кредитна мобільність	Відповідно до Положення про академічну мобільність студентів, аспірантів, докторантів, науково-педагогічних та наукових працівників ХНУМГ ім. О.М. Бекетова.
Міжнародна кредитна мобільність	Можливість участі в програмах міжнародної кредитної мобільності в рамках Erasmus+ International Credit Mobility з Близькосхідним технологічним університетом (м. Анкара, Туреччина), Лодзинським технічним університетом (м. Лодзь, Польща)
Навчання іноземних здобувачів вищої освіти	Відповідно до Правил прийому на навчання до ХНУМГ ім. О.М. Бекетова

2. Перелік обов’язкових компонентів освітньо-професійної/наукової програми та їх логічна послідовність

2.1. Перелік обов’язкових компонентів освітньої програми

Код ОК	Освітні компоненти (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Змістові модулі
1	2	3	4	5
Обов’язкові компоненти освітньої програми				
ОК 1.	Іноземна мова за професійним спрямуванням	7,0	залік, екзамен	*Модуль 1. Іноземна мова в соціальному аспекті* 1. - Іноземна мова у повсякденному житті 2. - Іноземна мова у вирішенні сучасних проблем соціуму. 3. - Іноземна мова в освітньому просторі. *Модуль 2. Іноземна мова в інформаційно-комунікаційному просторі* 4. - Міжкультурна комунікація в епоху глобалізації. 5. - Використання іноземної мови в роботі з інформаційно-комунікаційними технологіями. 6. - Іноземна мова у професійному середовищі.
ОК 2.	Філософія	4,0	екзамен	1. Історія філософії 2. Онтологія. Гносеологія 3. Соціальна філософія
ОК 3.	Українські історико-гуманітарні студії	3,0	зал	1. Суспільно-історичні особливості формування гуманітарного простору в Україні 2. Історико-культурні візії гуманітарної складової українського минулого
ОК 4.	Теорія і практика правозастосування	3,0	зал	1. Правові основи громадянського суспільства 2. Загальні засади реалізації конституційних прав і свобод людини та громадянина в Україні 3. Механізми захисту конституційних прав і

				свобод людини та громадянина
ОК 5.	Безпека життєдіяльності та основи охорони праці	4,0	диф. залік	1. Безпека життєдіяльності 2. Основи охорони праці
ОК 6.	Вища математика	9,0	диф залік, екзамен	*Модуль 1. Лінійна та векторна алгебра. Вступ до математичного аналізу. Інтегральне числення* 1. Лінійна алгебра та аналітична геометрія 2. Комплексні числа, елементарні функції, функції декількох змінних 3. Диференційне числення, інтегральне числення *Модуль 2. Диференціальні рівняння, ряди, операційне числення.* 4. Диференційні рівняння 5. Ряди 6. Операційне числення
ОК 7.	Фізика	4,0	диф залік	1. Механіка. Термодинаміка та молекулярна фізика 2. Електромагнетизм 3. Коливання і хвилі. Елементи атомної та ядерної фізики.
ОК 8.	Системи електронного документообігу	5,0	екзамен	1. Документальне забезпечення проектних робіт та управлінської діяльності 2. Електронний офіс як інформаційна модель організації 3. Організаційно-технологічні підходи до впровадження електронного документообігу
ОК 9.	Програмування	9,0	диф залік, екзамен	*Модуль 1. Вступ до програмування* 1. Поняття алгоритму та типові алгоритмічні структури програмування 2. Організація програм 3. Базові складові мови програмування високого рівня *Модуль 2. Технологія*

				проектування програм 4. Структури даних 5. Сортировка даних 6. Алгоритмізація типових обчислювальних задач
ОК 10.	Комп’ютерна графіка	5,0	екзамен	1. Вступ до комп'ютерної графіки 2. Технічне та програмне забезпечення комп'ютерної графіки. 3. Основні алгоритми комп'ютерної графіки
ОК 11.	Теорія ймовірностей та математична статистика	6,0	екзамен	1. Випадкові події. Системи випадкових величин. 2. Ймовірнісні процеси 3. Математична статистика. Задача вирівнювання статистичних рядів.
ОК 12.	UX-проєктування	5,0	диф. залік	1. HTML-мова розмітки веб сторінок. 2. CSS - мова дизайну веб сторінок 3. CMS – системи управління контентом
ОК 13.	Розробка клієнтських вебдодатків	4,0	диф. залік	1. Вступ до JavaScript. 2. Практичне використання JavaScript. 2. Етапи front-end розробки
ОК 14.	Інформаційні технології електронного бізнесу	5,0	екзамен	1. Складові електронного бізнесу 2. Інформаційні технології Internet для бізнесу 3. Інформаційні технології бізнес в internet-просторі
ОК 15.	Оптимізаційні методи та моделі	5,0	екзамен	1. Предмет та концепції математичного моделювання 2. Методи розв’язання оптимізаційних задач 3. Комп’ютерні системи для розв’язання оптимізаційних задач
ОК 16.	Архітектура комп'ютерних систем	5,0	екзамен	1. Комп'ютерна схемотехніка 2. Архітектура комп'ютерів 3. Зовнішні пристрої комп'ютерів
ОК 17.	Об'єктно-орієнтоване програмування	5,0	екзамен	1. Об'єктно-орієнтований аналіз та проектування. 2. Технологія об'єктно-орієнтованого програмування

				3. Об'єктно-орієнтоване програмування windows-застосувань
ОК 18.	Курсова робота "Об'єктно-орієнтоване програмування"	2,0	залік	1. Формулювання задачі та створення інфологічної моделі предметної області 2. Розробка та тестування програмних модулів 3. Підготовка і захист звіту
ОК 19.	Розробка серверних вебдодатків	5,0	екзамен	1. PHP - мова серверних сценаріїв. 2. Бази даних в веб-додатках. 3. Практичні завдання back-end розробки.
ОК 20.	Прикладні задачі дискретного аналізу	5,0	екзамен	1. Математичний апарат дискретного аналізу 2. Задачі дискретної оптимізації: постановка, властивості, обчислювальна складність. 3. Методи розв'язання задач дискретної оптимізації
ОК 21.	Організація баз даних та знань	4,0	диф. залік	1. Моделювання даних. 2. Мови запитів. 3. Проектування та захист баз даних.
ОК 22.	Курсова робота "Організація баз даних та знань"	2,0	залік	1. Формулювання задачі та створення інфологічної моделі предметної області 2. Створення бази даних і таблиць в СУБД. 3. Створення форм і запитів. Підготовка звіту
ОК 23.	Технології комп'ютерного проектування	5,0	екзамен	1. Складові електронного бізнесу 2. Інформаційні технології Internet для бізнесу 3. Інформаційні технології бізнес в internet-просторі
ОК 24.	Електротехніка та електроніка	4,0	залік	1 Функціональна схеми мікроконтролера. Основи програмування 2 Програмування порту, аналогового компаратора та аналого-цифрового перетворювача 3 Програмування таймера, прийомо-передавача та завантажувача програм.
ОК 25.	Основи електропостачання та	4,0	залік	1. Виробництво, передача

	електроспоживання			та розподіл електроенергії 2. Електричні та магнітні кола, машини, трансформатори 3. Електричні апарати в мережах, споживання електроенергії, безпека
ОК 26.	Цифрові підстанції	5,0	диф залік	1. Структура цифрової підстанції 2. Апаратна частина 3. Програмна частина
ОК 27.	Інформаційна безпека держави	4,0	диф залік	1. Задачі забезпечення інформаційної безпеки 2. Нормативна база у сфері інформаційної безпеки 3.Міжнародні стандарти та оцінка ризиків
ОК 28.	Основи технічного захисту інформації	5,0	диф залік	1. Поняття технічного захисту інформації 2. Основні етапи створення систем захисту інформації 3. Розробка політики безпеки інформації
ОК 29.	Алгоритми та структури даних	4,0	екзамен	1. Базові поняття про алгоритми 2. Структура даних 3. Методи розробки ефективних алгоритмів
ОК 30.	Курсова робота "Алгоритми та структури даних"	2,0	диф. захист	1. Розробка структурних схем модулів 2. Розробка програмної частини алгоритмів 3. Розробка, тестування та налагодження програми
ОК 31.	Криптографічний захист інформації	6,0	екзамен	1. Архітектура систем захисту інформації 2. Асиметричні криптосистеми захисту інформації 3. Сервіси і протоколи безпеки
ОК 32.	Криптоаналіз	5,0	екзамен	1. Загальні методи криптографії 2. Криптоаналіз шифрів підстановки 3. Криптоаналіз симетричних і поточних шифрів
ОК 33.	Комплексні системи захисту інформації об'єктів критичної інфраструктури	5,0	диф залік	1. Побудова критерії захищеності інформації 2. Системи виявлення та запобігання вторгнень

				3. Аналіз мережевої безпеки
ОК 34.	Моделювання процесів об'єктів критичної інфраструктури	5,0	диф залік	1. Моделі технологічних процесів 2. Розробка та аналіз політики безпеки 3.Кіберзахист об’єктів критичної інфраструктури
ОК 35.	Системи контролю доступу	6,0	екзамен	1. Об’єкти і суб’єкти доступу 2. Управління доступом до інформації 3. Політики доступу
ОК 36.	Технології виявлення вразливостей та вторгнень	5,0	диф залік	1. Мережева безпека 2. Загрози і джерела контролю загроз 3. Технології та протоколи захисту
ОК 37.	Навчальна практика	4,0	диф. захист	1. Використання офісних додатків у професійній діяльності (ПД), за матеріалами ресурсів IT-Academy). 2. Хмарні технології та засоби візуалізації у ПД 3. Використання комп’ютерної графіки та спеціалізованих онлайн-ресурсів у ПД.
ОК 38.	Виробнича практика	3,0	диф. захист	1. Аналіз і оцінка ризиків інформаційної безпеки 2. Організація комплексної безпеки об’єктів 3. Підготовка і захист звіту
ОК 39.	Єдиний державний кваліфікаційний іспит	1,0	екзамен	Відповідно до програми проведення іспиту
Загальний обсяг обов'язкових компонентів:		180		
Загальний обсяг вибіркових компонентів:		60		
ЗАГАЛЬНИЙ ОБСЯГ ПРОГРАМИ:		240		

Відомості про вибіркові компоненти наведені у додатку до освітньої програми.

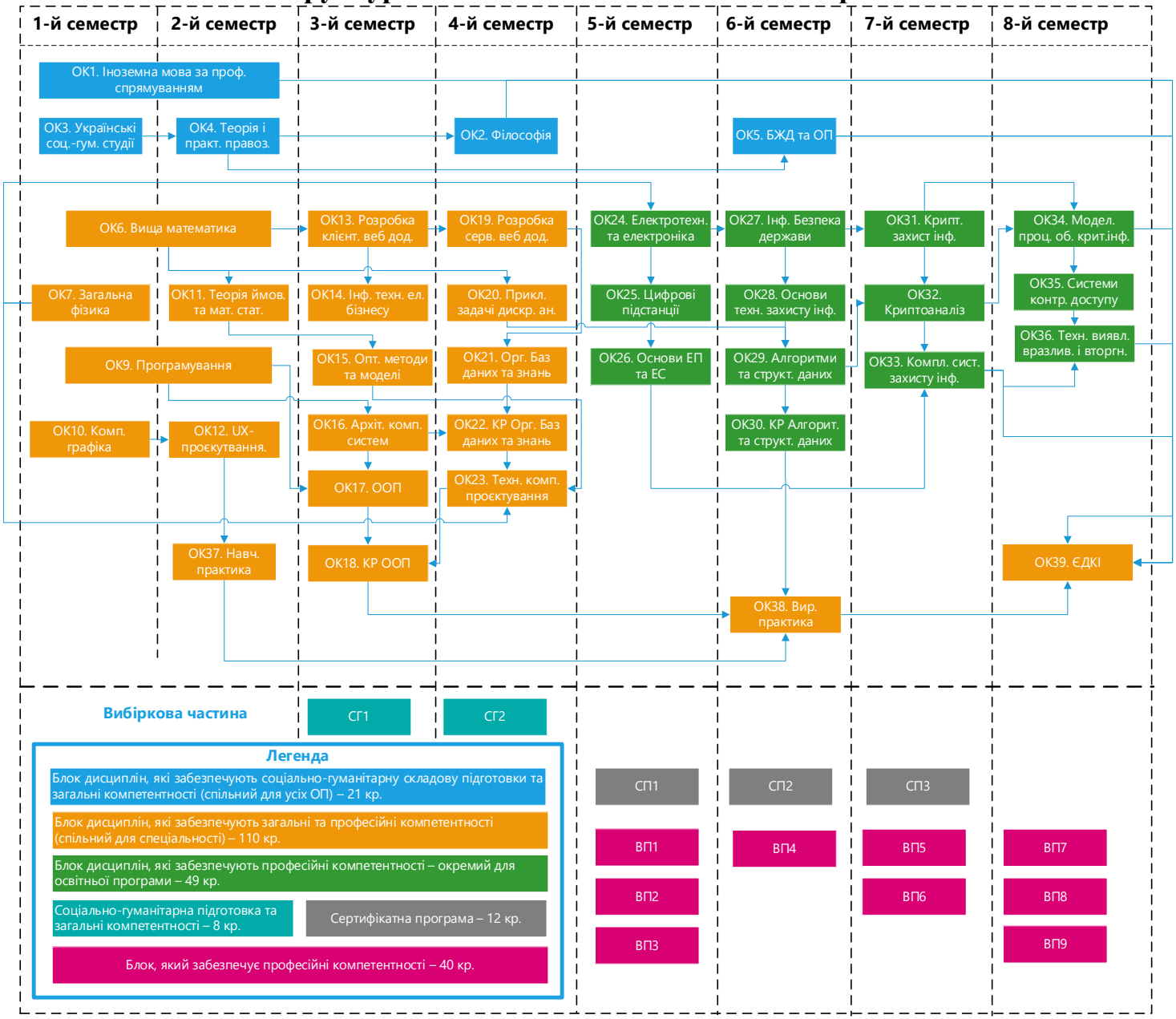
2.2. Структура освітніх компонентів за семестрами

Опис логічної послідовності вивчення компонент освітньої програми за семестрами

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
ОК1	ОК1	ОК13	ОК2	ОК24	ОК5	ОК31	ОК34
ОК3	ОК4	ОК14	ОК19	ОК25	ОК27	ОК32	ОК37
ОК6	ОК6	ОК15	ОК20	ОК26	ОК28	ОК33	ОК38
ОК7	ОК11	ОК16	ОК21		ОК29		
ОК8	ОК12	ОК17	ОК22		ОК30		
ОК9	ОК9	ОК18	ОК23		ОК36		

ОК10	ОК35						

Структура освітніх компонентів за семестрами



Розподіл обсягу (в кредитах ЄКТС) за обов'язковими та вибірковими освітніми компонентами за семестрами *на першому (бакалаврському) рівні*

Семестри	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Обов'язкові ОК	30	30	26	26	13	22	16	17
Вибіркові ОК	0	0	4	4	17	8	14	13
Разом за семестр	**30**	**30**	**30**	**30**	**30**	**30**	**30**	**30**

3. Форма атестації здобувачів вищої освіти

Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом спеціальності 125 Кібербезпека та захист інформації та освітньою програмою «Кібербезпека об'єктів критичної інфраструктури».

4. Матриця відповідності компетентностей освітнім компонентам освітньої програми

	ЗК1	**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**
ОК 1	•		•																
ОК 2	•					•	•												
ОК 3			•			•	•												
ОК 4						•		•											
ОК 5	•					•	•	•	•					•					
ОК 6	•								•										
ОК 7				•					•										
ОК 8					•			•	•										
ОК 9				•	•				•										
ОК 10	•				•														
ОК 11				•	•														
ОК 12										•	•								
ОК 13											•	•					•		•
ОК 14					•				•	•	•								
ОК 15				•	•														
ОК 16				•					•	•								•	
ОК 17	•				•			•							•				
ОК 18	•				•			•	•						•				
ОК 19				•								•					•		•
ОК 20								•	•										
ОК 21	•	•		•	•				•	•	•		•						
ОК 22	•	•		•	•				•	•	•		•						
ОК 23	•		•						•		•			•			•		
ОК 24	•			•															
ОК 25		•		•					•										
ОК 26	•	•		•					•										

	ЗК1	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
ОК 27						•		•							•	•			
ОК 28					•						•		•	•		•	•		
ОК 29				•					•	•									
ОК 30				•					•	•									
ОК 31	•	•		•					•	•		•					•		•
ОК 32				•	•												•		•
ОК 33		•									•	•		•		•		•	
ОК 34											•	•		•		•		•	
ОК 35								•	•							•			•
ОК 36				•					•	•		•			•				
ОК 37	•		•	•	•			•	•				•	•	•		•		
ОК 38	•																	•	•
ОК 39	•		•	•	•			•	•				•	•	•			•	

5. Матриця забезпечення програмних результатів навчання відповідними освітніми компонентами освітньої програми

ОК	ПРН1	ПРН2	ПРН3	ПРН4	ПРН5	ПРН6	ПРН7	ПРН8	ПРН9	ПРН10	ПРН11	ПРН12	ПРН13	ПРН14	ПРН15	ПРН16	ПРН17	ПРН18	ПРН19	ПРН20	ПРН21	ПРН22	ПРН23	ПРН24	ПРН25	ПРН26	ПРН27	ПРН28	ПРН29	ПРН30	ПРН31	ПРН32	ПРН33	ПРН34	ПРН35	ПРН36	ПРН37	ПРН38	ПРН39	ПРН40	ПРН41	ПРН42	ПРН43	ПРН44	ПРН45	ПРН46	ПРН47	ПРН48	ПРН49	ПРН50	ПРН51	ПРН52	ПРН53	ПРН54	ПРН55
1	•	•																																																					
2		•			•	•																				•																	•													
3		•																																																					
4							•																		•												•		•	•														•	
5										•														•																											•				
6					•	•															•																																		
7																										•	•						•																•						
8										•	•																																												
9													•		•			•	•	•																																				
10																						•								•			•		•																				
11										•	•	•																																												
12																														•			•		•																				
13													•		•			•	•	•																																			
14				•			•	•													•																																		
15			•	•																																																			
16		•	•											•		•	•																																						
17		•	•									•																			•		•																				
18		•	•									•																			•		•																				
19													•		•				•																																•				
20		•	•													•		•																																					
21		•	•											•										•																		•												
22		•	•											•										•																		•												
23					•							•						•																						•		•					•				•	
24															•											•														•		•						•			•	
25									•				•														•																								•			•	
26	•								•																																									•	•	•		•		
27							•																					•				•				•																		
28																	•						•														•	•	•		•					•						
29							•									•																•																•					•	
30							•									•																•																•						
31														•				•				•	•																										•				•			
32														•											•			•																									•			

ОК	ПРН1	ПРН2	ПРН3	ПРН4	ПРН5	ПРН6	ПРН7	ПРН8	ПРН9	ПРН10	ПРН11	ПРН12	ПРН13	ПРН14	ПРН15	ПРН16	ПРН17	ПРН18	ПРН19	ПРН20	ПРН21	ПРН22	ПРН23	ПРН24	ПРН25	ПРН26	ПРН27	ПРН28	ПРН29	ПРН30	ПРН31	ПРН32	ПРН33	ПРН34	ПРН35	ПРН36	ПРН37	ПРН38	ПРН39	ПРН40	ПРН41	ПРН42	ПРН43	ПРН44	ПРН45	ПРН46	ПРН47	ПРН48	ПРН49	ПРН50	ПРН51	ПРН52	ПРН53	ПРН54	ПРН55
33						•										•			•		•																							•											
34														•												•					•		•																						
35								•																																															
36				•					•						•			•						•										•														•						
37						•				•				•		•							•				•														•									•				
38								•						•						•				•																										•				
39																															•							•																