

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

УХВАЛЕНО

Рішенням вченої ради
Харківського національного
економічного університету
імені Семена Кузнеця
від 16.05.2025 р. протокол № 7

ВВЕДЕНО В ДІЮ

Наказом ректора Харківського
національного економічного університету
імені Семена Кузнеця
від 16.05.2025 р. № 160



Володимир ПОНОМАРЕНКО

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРБЕЗПЕКА»**

РІВЕНЬ ВИЩОЇ ОСВІТИ

Перший (бакалаврський)

СТУПІНЬ ВИЩОЇ ОСВІТИ

Бакалавр

ГАЛУЗЬ ЗНАНЬ

F Інформаційні технології

СПЕЦІАЛЬНІСТЬ

F5 Кібербезпека та захист інформації

Харків, 2025

ПРЕАМБУЛА

Робоча група освітньо-професійної програми «Кібербезпека»:

Лимаренко Вячеслав Володимирович, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук, гарант освітньої-професійної програми.

Шаповалова Олена Олександрівна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук, доцент.

Венгріна Олена Сергіївна, доцент кафедри кібербезпеки та інформаційних технологій, кандидат технічних наук.

Бойко Софія Олегівна, здобувач вищої освіти.

Губін Андрій Михайлович, Security Consultant, Engineering, GlobalLogic Ukraine.

Розглянуто на засіданні кафедри кібербезпеки та інформаційних технологій, протокол № 14 від 25.04.2025 року.

Розглянуто вченою радою навчально-наукового інституту інформаційних технологій, протокол № 10 від 28.04.2025 року.

ОП розроблена/оновлена на підставі:

1. Законодавчих та нормативних актів: Законів України «Про освіту», «Про вищу освіту», Національної рамки кваліфікації, Національного класифікатору України.

2. Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547.

3*На виконання Закону України «Про основи національного спротиву» від 16.07.2021 р. № 1702-IX, Постанови Кабінету Міністрів України «Про затвердження Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських» від 21.06.2024 р. № 734, листа МОН України «Про запровадження базової підготовки здобувачів вищої освіти» від 14.03.2025 р. № 1/4893-25.

4. Аналізу ринку праці, з урахуванням регіонального контексту.

5. Вивчення вітчизняного та зарубіжного досвіду.

6. Пропозицій роботодавців.

7. Рекомендації після процедур акредитації освітньої програми Національним агентством із забезпечення якості вищої освіти, протокол № 7 (50) від 27 квітня 2021 року.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузі знань	F Інформаційні технології
Спеціальності	F5 Кібербезпека та захист інформації
Спеціалізація	-
Освітня програма	Кібербезпека / Cybersecurity
Форми здобуття освіти, обсяг освітньої програми в кредитах ЄКТС та розрахункові строки виконання освітньої програми	На базі повної загальної середньої освіти: денна форма – 240 кредитів, 3 роки 10 місяців *243 кредити, 3 роки 10 місяців На базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст»): очна (денна) форма – 240 кредитів, 2 роки 10 місяців. *243 кредити, 2 роки 10 місяців
Наявність акредитації	Сертифікат про акредитацію освітньої програми НАЗЯВО № 1484, дійсний до 01.07.2026 р.
Мова(и) навчання / оцінювання	українська
Структурний підрозділ відповідальний за ОП	Кафедра кібербезпеки та інформаційних технологій; https://www.kafcb.it.hneu.edu.ua/
Вимоги до зарахування	Вступ на перший (бакалаврський) рівень вищої освіти здійснюється відповідно до Правил прийому та Порядку прийому на навчання для здобуття вищої освіти. Правила та строки прийому на навчання розміщені на сайті ХНЕУ ім. С. Кузнеця за посиланням https://pk.hneu.edu.ua/normatyvni-dokumenty/ Для успішного засвоєння освітньої програми бакалавра вступники повинні мати повну загальну середню освіту та прагнення оволодіти знаннями в галузі інформаційних технологій за спеціальністю кібербезпека та захист інформації.
Обмеження щодо форм навчання	Денна, заочна, дистанційна
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Кваліфікація(-ї) професійна(-і)	Відсутня
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – F5 Кібербезпека та захист інформації Освітня програма – Кібербезпека
Мета освітньої програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки.
Фокус та особливості (унікальність) програми	Особливістю ОПП Кібербезпека є орієнтація на сучасні вимоги до фахівців в галузі інформаційних технологій, та набуття здобувачами вищої освіти конкурентоспроможних компетентностей на основі синергізму отримання результатів навчання з інформаційної та/або кібербезпеки та програмування.
Опис предметної області	Об'єкти вивчення: технології кібербезпеки та захисту інформації; процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі

	інформаційні та Інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області: принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків), спеціалізований клас (кіберполігон).
Академічна мобільність	-
Академічні права	Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.
Професійні права	-
Працевлаштування випускників	Професії, на підготовку з яких спрямована ОП (згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010): адміністратор безпеки мереж і систем, 2139.2; фахівець сфери захисту інформації, 2139.2; фахівець з питань безпеки (Інформаційно-комунікаційні технології), 2139.2; конструктор систем кібербезпеки, 2132.2; фахівець з підтримки інфраструктури кіберзахисту, 2139.2; фахівець з реагування на інциденти кібербезпеки, 2139.2; фахівець з криптографічного захисту інформації, 2139.2; фахівець з технічного захисту інформації, 2139.2; фахівець з тестування систем захисту інформації, 2139.2; аудитор інформаційних технологій (з кібербезпеки), 2139.2; фахівець з оцінки заходів захисту інформації (кібербезпеки), 2139.2. А також на посади у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації
Силабуси освітніх компонентів	https://hneu.edu.ua/informatsijnyj-paket-bakalavr-kiberbezpeka-2025

II – ПЕРЕЛІК КОМПЕТЕНТНОСТЕЙ ВИПУСКНИКА

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК8. 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. ЗК15. Здатність захищати Батьківщину
Спеціальні (фахові, предметні) компетентності	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

	СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту Інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
--	---

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).

ІІІ – НОРМАТИВНИЙ ЗМІСТ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ, СФОРМУЛЬОВАНИЙ У ТЕРМІНАХ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗА СПЕЦІАЛЬНІСТЮ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ ОПІ «КІБЕРБЕЗПЕКА»

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

PH10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

PH11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

PH12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

PH13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

PH14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

PH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

PH16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

PH17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

PH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

PH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

PH20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

PH21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН22. Демонструвати готовність до захисту Батьківщини, володіючи системними знаннями з базової загальновійськової підготовки, опанувати основи військової справи, національної безпеки та оборони.

IV. СТРУКТУРА ОСВІТНЬОЇ ПРОГРАМИ ПІДГОТОВКИ БАКАЛАВРІВ

4.1. СТРУКТУРА ПРОГРАМИ ТА ОСВІТНІ КОМПОНЕНТИ

№	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Структура, %
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
1	ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ	23	10
2	ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ	25	10
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
3	ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ	157	65
4	ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ	35	15
Теоретична підготовка базової загальновійськової підготовки		3	
ЗАГАЛЬНА КІЛЬКІСТЬ:		240 (243)	100%
в тому числі: вибіркова складова		60	25

Код ОК	Освітні компоненти (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кредити ЄКТС	Форми підсумкового контролю
ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК 1	Українська мова (за професійним спрямуванням)	3	ЗАЛІК
ОК 2	Іноземна мова (за професійним спрямуванням)	9	ЗАЛІК, ЕКЗАМЕН
ОК 3	Історія української культури	4	ЗАЛІК
ОК 4	Філософія	5	ЕКЗАМЕН
ОК 5	Тренінг-курс «Безпека життєдіяльності та охорона праці»	2	ЗАЛІК
ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ			
ВК 1	Навчальна дисципліна правового спрямування	5	ЗАЛІК
ВК 2	Майнор або вільний майнор	5	ЗАЛІК
ВК 3	Майнор або вільний майнор	5	ЗАЛІК
ВК 4	Майнор або вільний майнор	5	ЗАЛІК
ВК 5	Майнор або вільний майнор	5	ЗАЛІК
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОБОВ'ЯЗКОВІ ОСВІТНІ КОМПОНЕНТИ			
ОК 6	Вступ до фаху	6	ЗАЛІК
ОК 7	Основи алгоритмізації	6	ЕКЗАМЕН
ОК 8	Вища математика	15	ЗАЛІК, ЕКЗАМЕН
ОК 9	Програмування	10	ЕКЗАМЕН, ЕКЗАМЕН
ОК 10	Дискретна математика	5	ЗАЛІК
ОК 11	Математичні основи криптології	4	ЗАЛІК
ОК 12	Основи побудови та захисту сучасних	5	ЕКЗАМЕН

	операційних систем		
ОК 13	Введення в мережі	5	ЕКЗАМЕН
ОК 14	Технології програмування	12	ЗАЛІК, ЕКЗАМЕН
ОК 15	Основи криптографічного захисту	5	ЕКЗАМЕН
ОК 16	Основи побудови та захисту мікропроцесорних систем	4	ЗАЛІК
ОК 17	Організаційне забезпечення захисту інформації	5	ЕКЗАМЕН
ОК 18	Основи математичного моделювання	4	ЗАЛІК
ОК 19	Розробка захищених мобільних застосунків	4	ЗАЛІК
ОК 20	Курсова робота: розробка захищених мобільних застосунків	1	КУРСОВА РОБОТА
ОК 21	Безпека в інформаційно-комунікаційних системах	5	ЕКЗАМЕН
ОК 22	Інформаційні системи та інтернет технології	12	ЕКЗАМЕН, ЕКЗАМЕН
ОК 23	Безпека інтернет-речей	6	ЕКЗАМЕН
ОК 24	Виробнича практика	3	ЗВІТ
ОК 25	Розробка захищених клієнт-серверних застосунків	4	ЗАЛІК
ОК 26	Курсова робота: розробка захищених клієнт-серверних застосунків	1	КУРСОВА РОБОТА
ОК 27	Іноземна мова академічної та професійної комунікації	4	ЗАЛІК
ОК 28	Комплексний курсовий проєкт	3	КОНСУЛЬТА- ЦІЙНИЙ ПРОЄКТ
ОК 29	Основи стеганографічного захисту інформації	4	ЗАЛІК
ОК 30	Хмарні технології та захист даних	4	ЗАЛІК
ОК 31	Комплексний тренінг	5	ЗВІТ
ОК 32	Переддипломна практика	5	ЗВІТ
ОК 33	Дипломний проєкт	9	ДИПЛОМНИЙ ПРОЄКТ
ОК 34	Єдиний державний кваліфікаційний іспит	1	ЄДКІ
<i>ВИБІРКОВІ ОСВІТНІ КОМПОНЕНТИ</i>			
ВК 6	Мейджор 1	5	ЕКЗАМЕН
ВК 7	Мейджор 2	5	ЕКЗАМЕН
ВК 8	Мейджор 3	5	ЕКЗАМЕН
ВК 9	Мейджор 4	5	ЕКЗАМЕН
ВК 10	Мейджор 5	5	ЕКЗАМЕН
ВК 11	Мейджор 6	5	ЕКЗАМЕН
ВК 12	Мейджор 7	5	ЕКЗАМЕН

БЗВП	ТЕОРЕТИЧНА ПІДГОТОВКА БАЗОВОЇ ЗАГАЛЬНОВІЙСЬКОВОЇ ПІДГОТОВКИ	3	Залік
------	---	---	-------

4.2. ВИБІРКОВА СКЛАДОВА ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Вибіркова складова навчального плану першого (бакалаврського) рівня вищої освіти складається з: вибіркової навчальної дисципліни за спрямуванням, майнора або вільних майнорів, мейджорів.

Здобувач вищої освіти обирає 1 майнор або 4 вільні майнори з загальноуніверситетського пулу дисциплін. Майнор, як правило, складається з 4 навчальних дисциплін. Обсяг кожної дисципліни майнора (вільного майнора) – 5 кредитів ЄКТС.

Як виняток, майнор може складатися з 2 навчальних дисциплін. Тоді, обсяг кожної дисципліни майнора – 10 кредитів ЄКТС. Дисципліни майнора (вільного майнора) викладаються по одній дисципліні в 3, 4, 5, 6 семестрах для здобувачів вищої освіти очної (денної) форми навчання. Формою підсумкового контролю дисциплін майнора (вільного майнора) є залік.

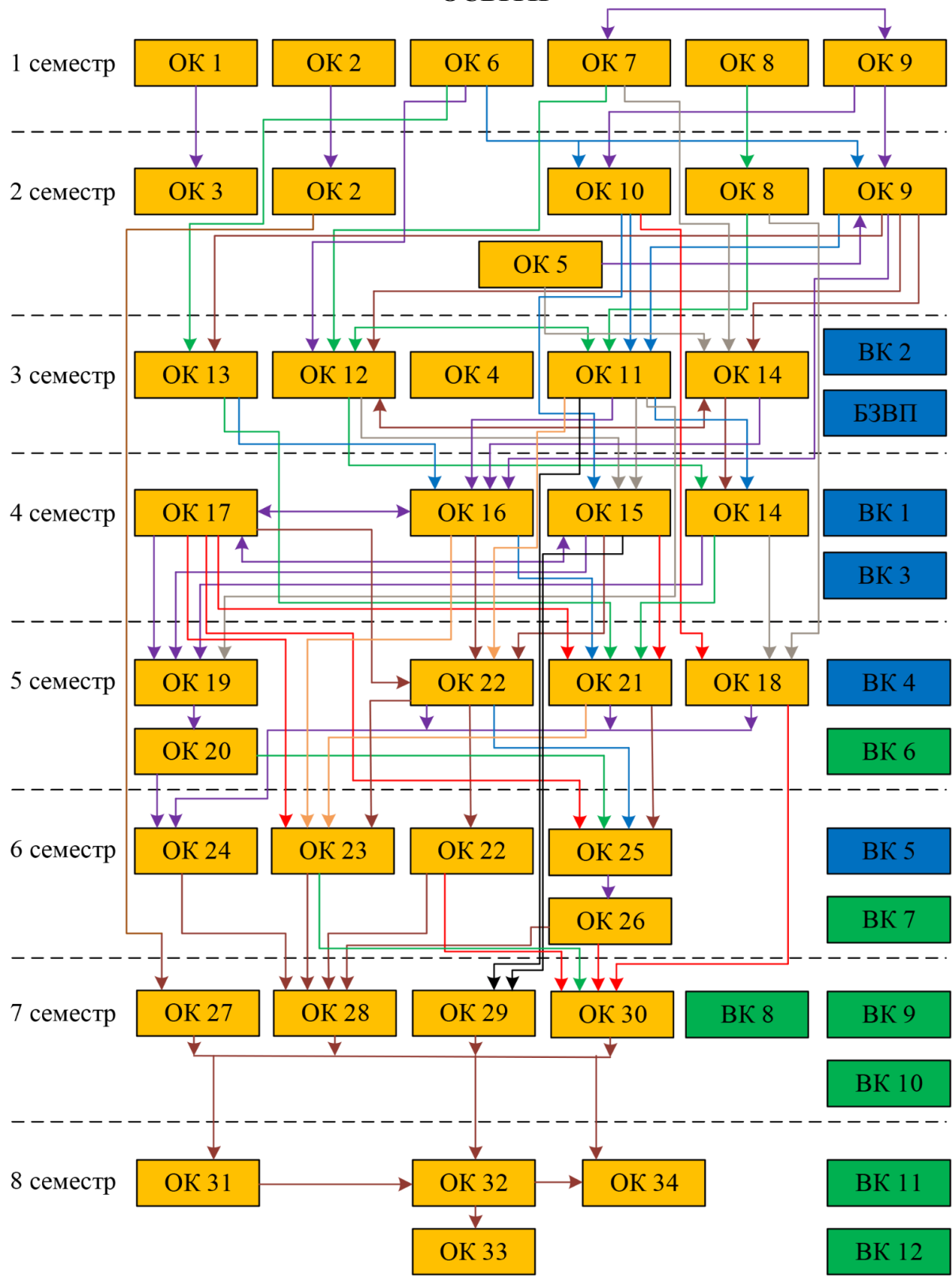
Здобувачеві вищої освіти пропонується обирати 1 дисципліну правового спрямування. Обсяг кожної вибіркової навчальної дисципліни за спрямуванням – 5 кредитів ЄКТС.

Формою підсумкового контролю за вибірковою навчальною дисципліною правового спрямування – залік.

Вибіркова навчальна дисципліна правового спрямування викладається в 3 або 4, або 5, або 6 семестрі для здобувачів вищої освіти очної (денної) форми навчання. Семестр, у якому викладається дисципліна, визначається навчальним планом освітньої програми.

Обсяг вибіркової навчальної дисципліни мейджора – 5 кредитів ЄКТС. Формою підсумкового контролю дисциплін мейджорів є екзамен (іспит). Дисципліни мейджори викладаються в 5, 6, 7, 8 семестрі для здобувачів вищої освіти очної (денної) форми навчання. Кількість дисциплін мейджорів, яка викладається в певному семестрі, визначається навчальним планом освітньої програми.

4.3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ



V. ФОРМИ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та дипломного проєкту.
Вимоги до єдиного державного кваліфікаційного іспиту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою.
Вимоги до кваліфікаційної роботи	Атестація за освітньою програмою здійснюється екзаменаційною комісією після виконання студентом навчального плану у формі публічного захисту кваліфікаційної роботи бакалавра (дипломного проєкту) за спеціальністю F5 Кібербезпека та захист інформації. Атестація осіб, які здобувають ступінь бакалавра, здійснюється екзаменаційною комісією (ЕК), до складу якої можуть включатися представники роботодавців та їх об'єднань. Атестація здійснюється відкрито і публічно. Дипломний проєкт – це робота здобувача, яка виконується на завершальному етапі здобуття кваліфікації бакалавра з кібербезпеки та захисту інформації для встановлення відповідності отриманих здобувачами вищої освіти результатів навчання (компетентностей) вимогам освітньої програми. 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. Дипломний проєкт є інструментом закріплення та демонстрації сформованих упродовж навчання загальних та спеціальних компетентностей відповідно до освітньо-професійної програми. У дипломному проєкті не повинно бути академічного плагіату, фальсифікації та фабрикації. Дипломний проєкт має бути оприлюднений (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.
Вимоги до публічного захисту	У процесі публічного захисту кандидат на присвоєння бакалаврського ступеня повинен показати уміння чітко і впевнено викладати зміст проведених досліджень, аргументовано відповідати на запитання та вести дискусію. Доповідь здобувача вищої освіти повинна супроводжуватися презентаційними матеріалами, призначеними для загального перегляду.

VI. 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».

Політика щодо забезпечення якості вищої освіти	Основні принципи внутрішнього забезпечення якості освіти у ХНЕУ ім. С. Кузнеця: відповідальності; відповідності; адекватності; автономності; вимірюваності; академічної культури; відкритості. Основні процедури внутрішнього забезпечення якості освіти в ХНЕУ ім. С. Кузнеця: формалізація політики якості, стратегічних цілей, завдань постійного поліпшення якості; забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації; забезпечення дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої освіти; підготовка та проведення маркетингово-моніторингових та соціально-психологічних досліджень для визначення потреб ринку праці, вимог стейкхолдерів вищої освіти, якості надання освітніх послуг і задоволеності якістю освітньої діяльності та якістю освіти; залучення стейкхолдерів вищої освіти (здобувачів вищої освіти, роботодавців, представників академічної спільноти тощо) до прийняття рішень за напрямками внутрішнього забезпечення якості; зовнішнє оцінювання якості діяльності ХНЕУ ім. С. Кузнеця за результатами участі в національних та міжнародних рейтингах вищих навчальних закладів, виконання Ліцензійних вимог, акредитації. Напрями: розроблення, затвердження, моніторинг та періодичний перегляд освітніх програм; забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; забезпечення студентоцентрованого навчання, викладання та оцінювання здобувачів вищої освіти; забезпечення наявності необхідних ресурсів для організації освітнього процесу; забезпечення наявності інформаційних систем для ефективного управління освітнім процесом.
Забезпечення якості розроблення, затвердження, моніторингу, перегляду та оновлення освітніх програм	Моніторинг та періодичний перегляд освітніх програм здійснюється згідно з діючими нормативними актами в ХНЕУ ім. С. Кузнеця. Перегляд освітніх програм здійснюється на основі аналізу задоволення освітніх потреб здобувачів вищої освіти: можливості побудови індивідуальної траєкторії навчання, дотримання академічних свобод в освітньому процесі, задоволеності якістю освітньої програми, тощо; роботодавців: якості формування загальних та фахових компетентностей, актуальних та соціальних навичок (soft skills); інших стейкхолдерів. Для перегляду освітніх програм використовуються: онлайн опитування, проведення дослідження фокус-групи, аналіз документів, аналіз ситуації, самооцінка робочою групою відповідно до вимог щодо структури та змісту освітньої програми.

	Періодичність перегляду освітніх програм здійснюється: а) щорічно за результатами моніторингу; б) після завершення освітньої програми здобувачами вищої освіти, в) в разі зміни законодавчої та нормативної бази.
Забезпечення зарахування, досягнення, визнання та атестація здобувачів	Оцінювання здобувачів вищої освіти є послідовним, прозорим та проводиться відповідно до встановлених в Університеті процедур згідно з нормативними актами. Щорічне оцінювання здобувачів освіти здійснюється відповідно до визначених освітньою програмою форм контролю; порядку оцінювання результатів навчання, що висвітлюється в робочих програмах навчальних дисциплін, робочих планах (технологічних картах) навчальних дисциплін, силабусах навчальних дисциплін; обліку результатів навчання, який ведеться з використанням програмного забезпечення корпоративної інформаційної системи управління (електронний журнал) та інформаційного середовища Персональної навчальної системи (ПНС) Університету. Оприлюднення результатів успішності, оцінювання результатів навчання відбувається через звіт «Інформація про поточну успішність та відвідування занять за навчальними дисциплінами семестру» (сайт Університету) та на сайті Персональних навчальних систем. Оцінювання здобувачів вищої освіти здійснюється на основі 100-бальної накопичувальної бально-рейтингової системи.
Забезпечення якості студентоцентрованого навчання, викладання та оцінювання	Планування, розподіл та надання навчальних ресурсів і забезпечення підтримки здобувачів вищої освіти враховують їх потреби та принципи студентоцентрованого навчання. Внутрішнє забезпечення якості вищої освіти гарантує, що всі необхідні ресурси відповідають цілям навчання, є загальнодоступними, а здобувачі вищої освіти поінформовані про їх наявність.
Забезпечення якості науково-педагогічних працівників	Щорічне рейтингове оцінювання діяльності науково-педагогічних працівників, кафедр і факультетів Університету здійснюється за рахунок використання механізмів оцінювання та самооцінювання результативності науково-педагогічної діяльності, її спрямованості на пріоритети розвитку національної системи вищої освіти, стратегії розвитку Університету, особистісного професійного розвитку науково-педагогічних працівників. Підсумки рейтингового оцінювання підводяться за результатами діяльності, досягнутими протягом навчального року. Оприлюднення результатів щорічного оцінювання науково-педагогічних працівників, кафедр та факультетів відбувається на засіданні вченої ради Університету.
Ресурсне забезпечення освітнього процесу (навчальні ресурси та підтримка здобувачів вищої освіти)	Заклад вищої освіти забезпечує освітній процес необхідними та доступними ресурсами (кадровими, методичними, матеріальними, інформаційними та ін.) та здійснює відповідну підтримку здобувачів вищої освіти. Організаційно-методична підтримка самостійної роботи здобувачів вищої освіти полягає у розробці методичних, дидактичних, інструктивних матеріалів, наданні можливості формувати, закріплювати, поглиблювати й систематизувати

	отримані під час аудиторних занять знання та вміння, здійснювати самопідготовку й самоконтроль опанування освітньої-професійної програми та реалізується через Персональну навчальну систему ХНЕУ ім. С. Кузнеця.
Інформаційне забезпечення (інформаційний менеджмент)	З метою управління освітнім процесом 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 організацію освітнього процесу; доступ до навчальних ресурсів; облік та аналіз успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; управління кадрами та ін.
Публічність інформації про освітні програми, освітню, наукову діяльність	Достовірна, об'єктивна, актуальна, своєчасна та легкодоступна інформація за освітньо-професійною програмою публікується на сайті ХНЕУ ім. С. Кузнеця, включаючи програми для потенційних здобувачів вищої освіти, випускників, інших стейкхолдерів і громадськості. Публічною є інформація про освітню діяльність за спеціальністю, включаючи критерії відбору на навчання; заплановані результати навчання за цією програмою; процедури навчання, викладання та оцінювання, що використовуються тощо.
Забезпечення академічної доброчесності	Забезпечення запобігання та виявлення академічного плагіату у наукових працях працівників закладу вищої освіти та здобувачів вищої освіти реалізується через політику, стандарти і процедури дотримання академічної доброчесності, регулюється такими документами ХНЕУ ім. С. Кузнеця: Кодекс академічної доброчесності; Кодекс професійної етики та організаційної культури працівників і здобувачів вищої освіти ХНЕУ ім. С. Кузнеця; Положення про комісію з питань академічної доброчесності ХНЕУ ім. С. Кузнеця. Перевірка наукових праць науково-педагогічних працівників Університету та здобувачів вищої освіти здійснюється за допомогою інтернет-сервісів на основі відкритих інтернет-ресурсів та системи StrikePlagiarism.com, що діє на підставі Ліцензійного Договору про надання права користування антиплагіатним програмним забезпеченням.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Матриця відповідності визначених компетентностей дескрипторам НРК та матриця відповідності визначених 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				
ЗК1. Здатність застосовувати знання у практичних ситуаціях.	+	+		
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.	+	+	+	
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.			+	
ЗК4. Здатність спілкуватися іноземною мовою.			+	+
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.	+	+	+	+
ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.	+		+	+
ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.			+	+
ЗК8. 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.	+		+	+
ЗК9 Здатність захищати Батьківщину	+	+	+	+
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
СК1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.	+	+	+	
СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.	+	+	+	
СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.		+		+
СК4. Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.		+		+

СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.		+	+	+
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).		+	+	+
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.		+	+	+
СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.	+	+		
СК9. Здатність застосовувати методи та засоби технічного захисту Інформації на об'єктах інформаційної діяльності.	+	+		
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.		+	+	+

Таблиця 2

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів

Результати навчання	Компетентності																		
	Загальні									Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	OK1		OK1 OK3 OK4		OK1 OK3 OK4			OK3 OK5		OK3 OK5									
РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.		OK2 OK27		OK2 OK27				OK2 OK27		OK2 OK27									
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.						OK6 OK17 OK21 OK23 OK28	OK6 OK17 OK21 OK23 OK28			OK6 OK17 OK21 OK23 OK28									
РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	OK5 OK12 OK13 OK16 OK19 OK20 OK25 OK26	OK5 OK6 OK12 OK13 OK25 OK26			OK25 OK26					OK5	OK12 OK13 OK25 OK26								
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.					OK7 OK9 OK30						OK9 OK30		OK9		OK7				OK14 OK30
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.		OK22			OK30						OK22 OK30		OK21	OK22	OK21	OK22		OK22	
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.					OK8 OK10						OK16 OK29	OK16			OK16 OK29	OK7	OK8 OK10 OK11 OK29		
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності,					OK8 OK10						OK18				OK8 OK10		OK8 OK10 OK11		

Результати навчання	Компетентності																		
	Загальні									Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.																			
РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.						OK6 OK17 OK21 OK23 OK28	OK6 OK17 OK21 OK23 OK28			OK6 OK17 OK21 OK23 OK28	OK6 OK17 OK21 OK23 OK28								
РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.	OK12 OK13 OK19 OK20 OK22 OK25 OK26 OK30	OK12 OK13 OK19 OK20 OK21 OK22 OK25 OK26 OK30									OK6 OK12 OK13 OK19 OK20 OK21 OK22 OK25 OK26 OK30		OK15 OK19 OK20 OK21 OK22 OK30	OK22	OK21 OK30	OK15 OK19 OK20 OK22		OK22	OK13 OK30
РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.		OK22 OK30 OK13									OK17 OK30	OK6	OK17 OK21						
РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.	OK22 OK30	OK12 OK19 OK20 OK22 OK30									OK12 OK22 OK30 OK31		OK31 OK21 OK22 OK30 OK12 OK19 OK20	OK21 OK22	OK21	OK22 OK30		OK22	
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.	OK22 OK30 OK13	OK22 OK30 OK13									OK12 OK13 OK19 OK20 OK25 OK26		OK21 OK22 OK30 OK12	OK21	OK21	OK19 OK20 OK25 OK26		OK22	OK12 OK19 OK20 OK25 OK26 OK30
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-											OK12		OK17 OK21	OK21	OK13 OK17 OK21				OK17

Результати навчання	Компетентності																		
	Загальні									Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.																			
PH15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.											OK13		OK17 OK21	OK21	OK17 OK21				OK14 OK17
PH16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	OK30	OK30								OK24 OK32	OK30	OK30	OK21 OK24 OK32	OK21 OK24 OK32	OK21 OK24 OK32			OK22	OK22 OK30
PH17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.		OK13											OK17 OK21	OK21	OK17 OK21				OK17
PH18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.					OK24 OK32								OK15 OK24 OK32				OK15 OK24 OK32	OK22 OK24 OK32	OK22 OK24 OK32
PH19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.					OK8 OK10 OK11 OK12 OK15								OK8 OK10 OK11 OK12 OK15				OK8 OK10 OK11 OK12 OK15		
PH20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.		OK13 OK16 OK17 OK21 OK23											OK13 OK16 OK17 OK21 OK23	OK13 OK16 OK17 OK21 OK23	OK13 OK16 OK17 OK21 OK23				OK13 OK16 OK17 OK21 OK23

Результати навчання	Компетентності																		
	Загальні									Спеціальні (фахові)									
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.											OK12 OK21 OK25 OK26				OK21	OK19 OK20 OK25 OK26			OK21
РН22. Демонструвати готовність до захисту Батьківщини, володіючи системними знаннями з базової загальновійськової підготовки, опанувати основи військової справи, національної безпеки та оборони.									БЗВП										

Гарант ОП

підписано

Вячеслав ЛИМАРЕНКО

ЛИСТ ПОГОДЖЕННЯ
Освітньо-професійної програми «Кібербезпека»

Назва структурного / функціонального підрозділу / посадова особа	Підпис
1. Навчально-методичний відділ	
2. Відділ забезпечення якості освіти	
3. Завідувач випускової кафедри	
4. Проректор з навчально-методичної роботи	

РЕЦЕНЗІЯ
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ
«КІБЕРБЕЗПЕКА»
ПЕРШОГО (БАКАЛАВРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ
ЗА СПЕЦІАЛЬНІСТЮ «F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЙ»
«ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ
ім. СЕМЕНА КУЗНЕЦЯ»

Компанія ЕРАМ є найбільшою та найвідомішою ІТ-компанією України. Вона впевнено очолює різні рейтинги за кількістю та якістю фахівців, які співпрацюють з компанією (понад 14 тис. фахівців). В той же час, в останні роки спостерігається тренд збільшення кількості та складності проектів, до яких долучаються фахівці компанії, що в свою чергу збільшує попит компанії на підготовку якісних фахівців. Рішення цього завдання компанія бачить у активній співпраці з навчальними закладами. З цього погляду підготовка якісних фахівців на кафедрі кібербезпеки та інформаційних технологій Харківського Національного Економічного Університету ім. Семена Кузнеця є актуальним завданням, що потребує тісної співпраці університету та компанії.

Можливості кафедри кібербезпеки та інформаційних технологій Харківського Національного Економічного Університету ім. Семена Кузнеця у підготовці якісних фахівців підкреслюються наявністю висококваліфікованого викладацького складу, серед яких можливо окремо виділити:

7 викладачів, що мають фаховий досвід співробітництва з провідними ІТ-компаніями або стартапами;

10 викладачів, що пройшли стажування у провідних ІТ-компаніях, та отримали відповідні сертифікати;

2 викладачів є сертифікованими фахівцями таких компаній як Microsoft, Google, Cisco, Oracle, AWS.

Харківський Національний Економічний Університет ім. Семена Кузнеця має відповідний досвід, розуміння культури інновацій, потужний кадровий потенціал та матеріально-технічну базу для виконання завдання підготовки ІТ-фахівців за обраним фокусом.

Проаналізувавши структуру програми та освітні компоненти, можна відзначити таке:

структура програми відповідає вимогам стандарту освіти у рамках спеціальності «F5 Кібербезпека та захист інформації»;

структурно-логічна схема підготовки здобувачів вищої освіти пройшла спільну верифікацію представниками кафедри та спеціалістами компанії ЕРАМ, що зафіксовано у відповідному протоколі засідання кафедри;

крім основних, стандартних форм навчання (лекції, практичні та лабораторні роботи, самостійна робота та ін.) у структурі програми передбачені інноваційні форми навчання, такі як самостійне та групове проектне навчання, комплексний

тренінг, IT-марафон.

Позитивною стороною освітньо-професійної програми є те що її розробка виконувалась співробітниками університету у співпраці з фахівцями компанії та IT-співтовариства:

зміст робочих програм та силабусів навчальних компонент «Технології програмування», «Основи стеганографічного захисту інформації» було верифіковано фахівцями компанії ЕРАМ, що зафіксовано у протоколі засідання кафедри;

побажання фахівців компанії щодо структурної та змістовної складових ОПП враховані та реалізовані у відповідних пунктах 4.1 та 4.3.

Висновки:

Зважаючи на позитивний досвід університету у підготовці фахівців, серед яких декілька осіб на поточний момент співпрацюють з компанією ЕРАМ та спираючись на результати рецензування вважаємо, що освітньо-професійна програма «КІБЕРБЕЗПЕКА» першого (бакалаврського) рівня вищої освіти за спеціальністю «F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ» ХАРКІВСЬКОГО НАЦІОНАЛЬНОГО ЕКОНОМІЧНОГО УНІВЕРСИТЕТУ ім. СЕМЕНА КУЗНЕЦЯ відповідає сучасним вимогам підготовки IT-фахівців та рекомендується до продовження терміну акредитації.

Заступник генерального директора
ТОВ "ЕРАМ СИСТЕМЗ"



Надія БАБЕЙКО

Рецензія

**на освітньо-професійну програму «Кібербезпека» за спеціальністю
F5 «Кібербезпека та захист інформації» першого (бакалаврського) рівня
вищої освіти в Харківському національному економічному університеті
імені Семена Кузнеця**

Ознайомившись з поданою на рецензування освітньо-професійною програмою «Кібербезпека» першого (бакалаврського) рівня вищої освіти в Харківському національному економічному університеті імені Семена Кузнеця можемо відзначити, що наповнення ОП відповідає визначеній цілі навчання щодо «підготовки фахівців, здатних використовувати й впроваджувати технології інформаційної та/або кібербезпеки, а також технологій цифрової економіки». Це чітко відповідає очікуванням ІТ-галузі щодо поєднання технічних компетенцій і цифрової грамотності.

Унікальність програми полягає в інтегруванні курсів з програмування та кібербезпеки, що формує конкурентоспроможні компетентності випускника, а можливість обирати майнор чи вільні майнори дозволяє студентам поглиблювати знання у суміжних галузях.

Позитивними сторонами освітньої програми є комплексність фундаментальної підготовки, що забезпечується такими освітніми компонентами, як математика, алгоритми, структури даних і програмування. Це створює міцний базис для розуміння алгоритмічних та криптографічних методів захисту даних. А також тим, що ОП охоплює класичні напрямки кібербезпеки (мережі, операційні системи, аудит безпеки, криптографія, управління інцидентами), що відповідає потребам найбільших ІТ-підприємств і державних структур. Наявність кіберполігону, курсових проєктів, переддипломної й виробничої практик забезпечує студентам безпосередній досвід застосування інструментів захисту інформації.

Тож, дана освітня програма вже має міцну основу, проте для її вдосконалення рекомендуємо розглянути певні напрями покращення. Це підвищить привабливість освітньої програми університету та сприятиме формуванню сильної школи кібербезпеки у Харкові.

Рекомендації щодо вдосконалення:

1. Впровадити курс «Методи машинного навчання в кібербезпеці» із практичними лабораторіями з аналізу аномалій та поведінкового виявлення загроз.
2. Посилити блок пентестингу та форензики окремим практикумом «Етичний хакінг» і «Цифрова криміналістика» з використанням Kali Linux, Metasploit та інструментів збору доказів.
3. Розвинути soft skills та підприємницькі компетенції через курс «Командна робота й ділова комунікація в ІТ», що включатиме презентаційні тренінги, переговорні кейси та основи кіберстартапів.

Загалом, програма «Кібербезпека» першого (бакалаврського) рівня вищої освіти в Харківському національному економічному університеті імені Семена Кузнеця має міцну фундаментальну базу, актуальні профільні дисципліни та добре організовану практичну підготовку, що відповідає вимогам ІТ-галузі та державних структур. Інтеграція програмування з курсами з кібербезпеки й можливість обирати майнори забезпечують конкурентоздатні компетенції випускників. Водночас впровадження курсів з машинного навчання в кібербезпеці, поглиблення навичок етичного хакінгу і цифрової криміналістики, а також розвиток soft skills і підприємницьких компетенцій зроблять програму ще більш привабливою та сучасною. Реалізація цих рекомендацій сприятиме подальшому зміцненню позицій ХНЕУ ім. С. Кузнеця як провідного центру у підготовці фахівців з кібербезпеки в регіоні.

Виконавчий директор
ГС «Харківський кластер
інформаційних технологій»

2025 рік



Ольга ШАПОВАЛ



ТОВ «Спарта Роботек»
Україна, 61072, Харківська обл.,
м. Харків,
вул. Олеса Олександра, б. 10
к.т. +38067-972-7000
spartarobotech@gmail.com

РЕЦЕНЗІЯ-ВІДГУК

**на освітньо-професійну програму «Кібербезпека»
спеціальності F5 Кібербезпека та захист інформації
першого (бакалаврського) рівня вищої освіти
у Харківському національному економічному університеті ім. С. Кузнеця**

Кібербезпека – це сукупність процесів, технологій і практик, спрямованих на захист комп'ютерних систем, мереж, програм, пристроїв і даних від несанкціонованого доступу, кібератак, пошкоджень або знищення. Кібербезпека є критично важливою для державних установ, підприємств, банків, медичних закладів та будь-яких організацій, які працюють з конфіденційною інформацією. В умовах війни, яка ведеться проти нашої держави в тому числі і на інформаційному фронті, важко переоцінити важливість кібербезпеки, як напрямку підготовки ІТ-спеціалістів.

Освітня програма «Кібербезпека», що реалізується на кафедрі Кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця, є однією з найсильніших у регіоні за глибиною, практичною цінністю та сучасністю змісту.

Програма повністю відповідає викликам часу й орієнтована на підготовку висококваліфікованих фахівців, здатних ефективно працювати в умовах зростаючих кіберзагроз як у державному, так і в приватному секторі.

Особливо варто відзначити:

- комплексний підхід до навчання – студенти отримують знання з технічного захисту інформації, криптографії, управління інформаційною безпекою, кіберрозвідки, цифрової криміналістики та інших важливих напрямів;

- високий рівень викладацького складу – викладачі кафедри мають глибокі наукові знання, практичний досвід та тісні зв'язки з ІТ-індустрією й безпековими структурами;

- сучасна матеріально-технічна база – навчальні лабораторії оснащені всім необхідним для моделювання кіберінцидентів, аналізу загроз та проведення практичних занять;

- практична орієнтованість – студенти залучаються до участі в хакатонах, наукових конференціях, проходять стажування в ІТ-компаніях і профільних установах, зокрема у сфері державної безпеки.

Програма не лише формує ґрунтовні технічні компетентності, а й розвиває критичне мислення, навички командної роботи та аналітичного підходу до вирішення проблем.

Рекомендуємо освітню програму «Кібербезпека» спеціальності F5 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти, що провадиться на кафедрі Кібербезпеки та інформаційних технологій ХНЕУ ім. С. Кузнеця, всім, хто прагне здобути актуальну професію з великим майбутнім і зробити свій внесок у безпеку цифрового суспільства.

Директор ТОВ
«Спарта РобоТек»



Наталія ХИЖНЯК

РЕЦЕНЗИЯ

**на освітньо-професійну програму «Кібербезпека»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 - Кібербезпека
галузі знань F - Інформаційні технології**

Харківського національного економічного університету ім. Семе́на Кузне́ця

У сучасних умовах цифровізації зростає потреба у фахівцях з кібербезпеки, які володіють фундаментальними знаннями та практичними навичками. Представлена ОПП «Кібербезпека» бакалаврського рівня Харківського національного економічного університету ім. Семе́на Кузне́ця орієнтована на формування базових компетенцій, необхідних для роботи в ІТ-безпеці.

Програма охоплює такі ключові напрями:

- основи інформаційної безпеки та захисту даних;
- адміністрування комп'ютерних мереж і виявлення вразливостей;
- базові принципи криптографії та захисту програмного забезпечення.

Навчальний план включає як теоретичні дисципліни, так і практичні модулі, що сприяє засвоєнню знань та формуванню професійних навичок.

ОПП «Кібербезпека» відповідає сучасним стандартам освіти та забезпечує необхідний рівень підготовки для подальшого навчання або роботи в галузі кібербезпеки.

ОПП містить перелік навчальних компонентів та опис їх логічних зв'язків, матрицю забезпечення результатів навчання компонентами ОПП, визначення форми атестації здобувачів. Це дозволяє зробити висновок про зміст навчання за ОПП.

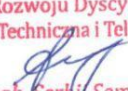
ОПП «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю F5-Кібербезпека галузі знань F-Інформаційні технології Харківського національного економічного університету ім. Семе́на Кузне́ця є актуальною, відповідає вимогам підготовки здобувача вищої освіти рівня бакалавр.

Професор кафедри комп'ютерної інженерії та кібербезпеки
Університет комісії Національної світи в Кракові (Польща)



д.т.н. Анна КОРЧЕНКО

Pełnomocnik Rektora
ds. Rozwoju Dyscypliny
Informatyka Techniczna i Telekomunikacja



dr hab. Serhiy Semenov